NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

MARINE GROUND INTELLIGENCE REFORM:
HOW TO REDESIGN GROUND INTELLIGENCE FOR THE
THREATS OF THE 21ST CENTURY

by

Drew E. Cukor

December 1997

Thesis Advisor: Nancy Roberts
Associate Advisor: Erik Jansen

Approved for public release; distribution is unlimited.

DTIC QUALITY INSPECTED

19980414 113

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 1997	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE MARINE GROUND INTELLIGENCE REFORM: HOW TO REDESIGN GROUND INTELLIGENCE FOR THE THREATS OF THE 21ST CENTURY	5. FUNDING NUMBERS
6. AUTHOR(S) Cukor, Drew E.	

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

Present-day Marine ground intelligence is configured for attrition warfighting and the predictable conventional adversaries of the past. Designed during WWII, it has undergone little change; what has changed is the threat environment. Modern-day threats are less centralized and regimented. They think on their own and they adapt quickly. This thesis analyzes the current configuration of Marine ground intelligence and compares it with two major threats of the next century: asymmetric military threats and non-conventional threats. To counter these smart adversaries, Marine ground intelligence will need to be configured differently. Sophisticated sensors and rote intelligence work are no longer enough to identify and track these powerful threats. The performance of Marine intelligence during the Gulf War demonstrates that having failed against the Iraqi army, intelligence is very likely to fail again. Indeed, Marine intelligence faces a serious dilemma: it can either reform or face ever-decreasing relevance and effectiveness. Having presented the rationale for urgent reform, this work recommends an intelligence enterprise centered around the leveraging of human intellect. It suggests the network as the design change that best leverages intellect and optimally configures ground intelligence for operating successfully against the threats of the next century.

14. SUBJECT TERMS Ground Intelligence, Intelligence Reform, Maneuver Warfare, Attrition Warfare, The Gulf War, Operation Restore Hope, UNOSOM II, Asymmetric Military Threats, Emerging Non-Conventional Threats, Network Intelligence, Virtual Intelligence.	15. NUMBER OF PAGES 230
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

MARINE GROUND INTELLIGENCE REFORM:
HOW TO REDESIGN GROUND INTELLIGENCE FOR THE THREATS OF THE 21ST CENTURY

Drew E. Cukor
Captain, United States Marine Corps
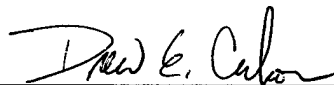B.A., University of Southern California, 1992

Submitted in partial fulfillment of the
requirements for the degree of

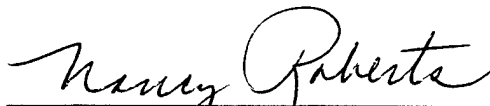## MASTER OF SCIENCE IN SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
December 1997

Author: _____
Drew E. Cukor

Approved by: _____
Nancy Roberts, Thesis Advisor

_____
Erik Jansen, Associate Advisor

_____
Rubin Harris, Chair
Department of Systems Management

iv

ABSTRACT

Present-day Marine ground intelligence is configured for attrition warfighting and the predictable conventional adversaries of the past. Designed during WWII, it has undergone little change; what has changed is the threat environment. Modern-day threats are less centralized and regimented. They think on their own and they adapt quickly. This thesis analyzes the current configuration of Marine ground intelligence and compares it with two major threats of the next century: asymmetric military threats and non-conventional threats. To counter these smart adversaries, Marine ground intelligence will need to be configured differently. Sophisticated sensors and rote intelligence work are no longer enough to identify and track these powerful threats. The performance of Marine intelligence during the Gulf War demonstrates that having failed against the Iraqi army, intelligence is very likely to fail again. Indeed, Marine intelligence faces a serious dilemma: it can either reform or face ever-decreasing relevance and effectiveness. Having presented the rationale for urgent reform, this work recommends an intelligence enterprise centered around the leveraging of human intellect. It suggests the network as the design change that best leverages intellect and optimally configures ground intelligence for operating successfully against the threats of the next century.

TABLE OF CONTENTS

I. INTRODUCTION

A.   GENERAL STATEMENT OF THE PROBLEM

Present-day Marine Corps ground intelligence is a product of the industrial age. It is configured for the predictable, conventional adversaries of the past. Designed during WWII, it has undergone little change since.

This thesis examines the critical need for dramatic structural change in Marine Corps ground intelligence operations and suggests an alternative, intellect-centric, network enterprise designed to meet the demands of the next century.

What is the basis of this call for change? Now more than ever, Marine combat forces face a spectrum of threats that present grave challenges to future ground operations. In the Gulf War, intelligence was unable to provide suitable ground intelligence to tactical commanders against the Iraqi army. Despite urgent calls from battlefield commanders and intelligence professionals alike, little has been done to modify intelligence practices and organizational design; in fact, Marine ground intelligence has remained fundamentally unchanged in the seven years since the Gulf War.[1] Even efforts to incorporate automated information systems have not stirred reexamination of operating practices and organization. Accepting current practices and

---

[1]This work recognizes that a series of changes to Marine intelligence have occurred since the conclusion of the Gulf War. Most notably after the completion of a study by the Department of Defense inspector general, a mission area analysis, and the work of the Marine Corps Executive Steering Group, six specific areas were highlighted for improvement. They were inadequate doctrinal foundation, insufficient tactical intelligence support, lack of professional intelligence officer career development, insufficient joint manning, insufficient language capability and inadequate imagery capability. From (FY) 1995-1997 each of these deficiencies were systematically addressed and corrective action taken. While these improvements are important, they have only been incremental, peripheral changes. This thesis argues that the fundamental processes that transform raw data into useable knowledge or intelligence have not changed since WWII. Incremental manning, training, or career enhancement changes are not solutions to this wider problem and therefore are seen as minor adjustments to an enterprise that still is wedded to practices of the industrial age.

design as sound, management information system (MIS) efforts have done little more than automate existing procedures.[2] The results of these actions can be seen in ground exercises throughout the Marine Corps in which intelligence continues to fail combat decision-makers.[3]

While intelligence has remained unchanged and tied to outdated processes and design, Marine warfighting doctrine has undergone significant transformation. Seeking a framework for fighting wars that is consistent with the emerging threat environment, the Marine Corps has abandoned warfare of attrition and adopted instead maneuver warfare. Yet, in spite of this transition, experiences in the Gulf War demonstrate that intelligence repeatedly failed to provide the intelligence required to operate in the maneuverist paradigm. Careful study shows that Marine ground intelligence was organizationally unable to provide the detail of information age intelligence demanded by combat decision-makers facing the Iraqi army. This analysis highlights the mismatch between maneuver warfare and existing Marine intelligence operations, one of the major weakness of the current intelligence organization.

Indeed, Marine intelligence faces a serious dilemma: it can either reform or face ever decreasing relevance and effectiveness. Unless significant reform is realized,

---

[2] The intelligence analysis system or IAS is the Marine Corps' intelligence information management system. It has been in development since before August of 1991 and is presently fielded at the Marine Expeditionary Force (MEF) G-2 (intelligence) level. The mission of IAS is to automate intelligence activities like directing collecting, processing and disseminating combat intelligence in order to rapidly analyze, produce and disseminate all-source intelligence. IAS does not change doctrine or fundamental intelligence activities that convert raw data into useable intelligence. Rather, IAS automates preexisting tasks and reinforces traditional intelligence practices by replacing manual processes with an automated management information system (MIS).

[3] The fundamental intelligence question that combat decision-makers repeatedly ask is "where is the enemy?" The author spent three years as an intelligence officer of a Marine Infantry Battalion from (1992-1996) and could rarely answer this using quantitative data, like imagery, or "hits" from other information age sensors. Identifying the enemy's disposition is critical to successful intelligence work. Yet, this is a task that continues to be troublesome for Marine intelligence. Until this detail of intelligence can be

intelligence as a fundamental component of command and control on the battlefield will fail decision-makers facing emerging twenty-first century threats.

B. PURPOSE OF THE WORK

This thesis is about the misalignment of intelligence with its environment. As this work will demonstrate, the structure of Marine ground intelligence is that of a machine bureaucracy: centralized, hierarchical and slow. Marine intelligence is designed to accommodate attrition warfighting and simple predictable adversaries; it is severely challenged when confronted with the demands of maneuver warfare and non-standard, unpredictable adversaries.

Ill configured for threats like the Iraqi Army, Marine ground intelligence will assuredly fail against emerging twenty-first century threats.   So far, disaster has been averted by the individual innovation and "get the job done" attitude of intelligence personnel. Yet these "quick fixes" are rarely formalized by the organization. There is generally an official way to do intelligence and then there is the way things are actually done. It is the largely informal, ad-hoc actions of innovative intelligence professionals that have dealt with recent challenges, but the dictates of the machine bureaucracy still permeate the organization. The restrictive boundaries, formalized processes, regimented hierarchical approach to collections and dissemination, and the centralization of assets and resources prevents Marine ground intelligence from exploiting its full potential and effectively performing its critical mission. Unless intelligence adapts its structure and processes to meet the demands of its environment it faces irrelevance as a component of

---

provided seamlessly to decision-makers, intelligence will continue to fail at its primary mission; to provide combat decision makers with the knowledge necessary to make informed decisions about an enemy.

command and control on the battlefield.

C.   RESEARCH QUESTIONS

This paper seeks to answer three broad questions. First, what is the emerging threat environment of the twenty-first century? Second, is the present Marine ground intelligence design adequate to support combat decision-makers in this threat environment? Third, if not, what design changes are necessary to align intelligence with this environment?

D.   METHODOLOGY

This study is a conceptual analysis that draws on case studies to describe and prescribe how Marine ground intelligence should be configured as it enters the next century. It uses the methods of the futurists by identifying important trends and projecting what the future may look like. This work analyzes current military and economic trends to project what the threat environment will mean for current ground intelligence practices. It then breaks down the current ground intelligence design and compares it with this environment to demonstrate the misalignment between the two. Drawing on industry examples and academic research this work recommends how intelligence should be reconfigured to better align itself with the emerging threat environment.

E.   STRUCTURE OF THE THESIS

The goal of this thesis is to highlight the inadequacy of the present-day Marine ground intelligence organization and to suggest an alternative configuration that is aligned with the environment this organization will face in the coming century. Before the reader can truly appreciate the implications of the emerging threat environment

4

described in later chapters of this thesis, it will be essential to acquire an adequate background on the current structure and functioning of Marine ground intelligence. Chapter II, therefore, sets up the current problem with intelligence by demonstrating the failure of Marine ground intelligence in the Gulf War. This discussion helps the reader identify the misalignment between modern ground intelligence practices and the warfighting doctrine of the Marine Corps. It supports the argument that intelligence will most likely fail against emerging twenty-first century threats given its performance in the Gulf War.

Chapter III continues this discussion by presenting an overview of the organizational design of existing Marine Corps intelligence. Additionally, it provides an evaluation of elements of the intelligence bureaucracy, emphasizing that the organizational design, by its very nature, lacks effectiveness and is limited in its ability to respond to New Order Threats.

After orienting the reader to contemporary Marine intelligence operations, this thesis focuses on an in-depth exploration of the major threats of the next century: asymmetric military threats and emerging non-conventional threats. Chapters IV through VI will make startlingly clear the imperative for change in Marine intelligence by providing evidence compiled from recently collected data on a wide range of topics, such as global military spending, U.S. gang activity, and world refugee population statistics, as well as an analysis of case studies from actual and hypothetical military encounters in Somalia and China, respectively.

The common thread woven throughout this rationale for change is the premise that asymmetric and emerging non-conventional threats are posing greater complexity

5

and danger for the Marine Corps than threats of the past. These emerging *New Order Threats* require that significant and immediate attention be paid to the need for Marine intelligence reform.

Having presented the rationale for why Marine intelligence needs to change, the final and most important chapter of this thesis recommends the direction and types of particular reforms mandated by maneuver warfare and emerging New Order Threats. Applying lessons learned from the private sector and from organizational theory it argues that the development and deployment of intellect is the key to successful ground intelligence. It further argues that successfully leveraging intellect demands an organizational design that pushes responsibility outward, flattens and removes hierarchy, and exploits a wide range of expertise within and outside of the military. The network organization is the form that best does this. Accordingly, network based intelligence is suggested as the model for intelligence reform.

F.   NEW ORDER THREATS

For purposes of this thesis, the term *New Order Threat* is used to capture the two primary challenges that threaten Marine combat operations in the next century. First are asymmetric military threats. Defined in Chapter IV as an evolving form of twentieth century conventional war, asymmetric military threats attempt to circumvent Western conventional superiority. Pushed into new forms of warmaking because of U.S. conventional dominance, they seek asymmetry to overcome American military and technological dominance. The second is the emerging class of non-conventional threats. As explained in Chapter V and VI these emerging threats harness inherent organizational asymmetries to circumvent American conventional dominance. They are no longer a

6

phenomenon of developing nations. Indeed, they are appearing throughout the modern

world. Together these two powerful threats represent a *New Order of Threats* that

promise to severely challenge American military dominance in the twenty-first century.

New Order Threats challenge American military dominance because they are difficult to

recognize and understand. As a result decision-makers delay or respond ineffectively.

Left unchecked *New Order Threats* harness powerful asymmetric capabilities that allow

them to gain influence that is out of proportion to their political, economic and military

strength.

G.   FOCUS OF STUDY

The thesis focuses on only one facet of Marine Corps intelligence: ground

intelligence. The other components, air intelligence, signals intelligence and human

intelligence are not studied specifically but are included in the body of the work as they

relate to the ground intelligence effort. Ground intelligence is the focus of this work

because the Marine Corps is essentially a ground force. The Marine Corps is

fundamentally an air-ground, combined-arms team. It is the maneuver and fire of ground

forces operating in conjunction with close air support, naval surface fires and artillery

that place our adversaries in a position from which they have few choices. Therefore,

ground intelligence is critical to all Marine operations. If ground intelligence cannot

provide knowledge on the enemy, the entire air-ground, combined arms team is effected.

Accordingly, as the center for all Marine intelligence operations, ground intelligence is

taken as the critical element for reform.

II. WHY CHANGE MARINE GROUND INTELLIGENCE?

A. MARINE GROUND INTELLIGENCE AND THE GULF WAR

This chapter will frame the need for intelligence reform by demonstrating the

failure of Marine intelligence during the Gulf War. The broader implications of these

failures coupled with similar failures of Army intelligence will then be used to expose the

central cause for the escape of the Iraqi Republican Guard Divisions prior to the

conclusion of the war. This discussion serves to highlight the dim prospects present-day

Marine intelligence holds for operating successfully against the emerging threat

environment of the twenty-first century; it also initiates the reader to the study of the

emerging threat environment, presented in later chapters, that provides a true sense of the

intelligence requirements needed as the Marine Corps enters the twenty-first century.

B. CHANGE IN MARINE WARFIGHTING DOCTRINE

During the Gulf War a new information era for the military came of age, and

ground commanders demanded information age intelligence. At the same time,

warfighting doctrine also changed.

With the conclusion of the Vietnam War, the American military had begun a

transformation that manifested itself during the Gulf War as a new, high technology

force. Extremely sensitive to public opinion, this military transformation witnessed the

development of weapon systems and warfighting doctrine that were designed to reduce

collateral damage and friendly casualties. The impetus for this transformation was the

Congress' and American society's changing attitudes towards the military. The American

military could no longer count on a limitless spending and labor pool. The draft had

ended in the early 1970s, and training was an expensive and time-consuming process. Furthermore, defense budgetary oversight by the Congress and shrinking defense expenditures forced DoD into conservative approaches toward spending and defense infrastructure. In short, in order to overcome the constraints imposed by the Congress and American society, the military abandoned warfare by attrition. Military victory would need to come through military competence, not from sheer superiority of men and material as it had in previous conflicts.

The Marine Corps' response to the military transformation was made evident in the adoption of warfare by maneuver. As shown in Table 2.1, attrition warfare demands numerical and technological superiority for success, while maneuver warfare applies strength against selected enemy weaknesses. Attrition warfare calls for the wearing down of each individual component of the enemy system, while maneuver warfare relies on speed, surprise, and the application of strength at the right time and place to shatter an enemy's logic.

	Attrition Warfare	Maneuver Warfare
Style of Maneuver	Movement to Contact	Deliberate Attack
Resource requirements	Vast labor and weapons pool	Highly trained personnel and high technology weapons
Key to success	Numerical and technological superiority over enemy	Precise intelligence about enemy weakness
Indicator of success	Destruction of all enemy units	Destruction of enemy logic

Table 2.1. Attrition vs. Maneuver Warfare.

Maneuver warfare allows components of the enemy system to remain untouched, for it is the shattering of the enemy's logic or "raison d'etre" that renders him incapable of

10

functioning as a cohesive entity. Thus the destruction of that logic through violent contact creates a situation in which the enemy cannot cope and his ability to fight is paralyzed. Maneuver warfare success is achieved by shattering the enemy's cohesion, organization, command and control, and physiological balance, not by physically destroying each enemy unit. It is through maneuver warfare that an inferior force can achieve decisive superiority by applying overwhelming force at the necessary time and place.

Unlike attrition warfare, where firepower and movement are massed to incrementally reduce the enemy's strength, maneuver warfare is designed to counter threats that are ambiguous and numerically superior. While maneuver warfare accepts and thrives on the chaotic and uncertain battlefield of the future, it demands precise intelligence. Fundamental to warfare by maneuver is circumventing enemy strengths and attacking from a position of advantage rather than head-on. As a result, successful maneuver depends on the ability to identify and exploit enemy weaknesses. This is not a trivial task; it requires complex intelligence work. Intelligence, therefore, is a key element in the successful application of maneuver warfare on the battlefield.

Ground combat leaders cannot collapse an enemy's logic or shatter its cohesion if they do not know where to inflict such violent blows. Yet, Marine intelligence is not configured to meet the demands of maneuver warfare. Indeed, we will see that Marine intelligence failed even to support attrition warfare during the Gulf Conflict. Left without intelligence on the enemy, commanders attacked forward, unaware as to enemy strengths and intentions. Fortunately, the Iraqi Army proved weak and irresolute, and American combat power defeated the enemy without the need for precise intelligence. However,

11

the future promises to be much different. A similar failure may provide future threats with unprecedented battlefield advantages, the repercussions of which could pose serious challenges for Marine combat forces.

1.   Movement to Contact vs. the Deliberate Attack

The Gulf War provides an outstanding backdrop to highlight Marine ground intelligence's failure to provide battlefield commanders intelligence on enemy dispositions and intentions. This failure led to the Marine's heavy use of movement to contact operations, rather than the deliberate attack characteristic of maneuver warfare.

Representing the quintessential twentieth century conventional force, Saddam Hussein's military was centralized, regimented, and very conventional. His army was the adversary which Marine intelligence had been designed to operate optimally against. Furthermore, the desert was the perfect terrain to support offensive operations. Flat, bare, and open, the desert was an environment where American technology and intelligence collection systems could be harnessed to their full potential.

Unfortunately, Marine ground intelligence did not enter the Gulf War configured to provide the critical battlefield intelligence needed to support maneuver warfare. Because of this, offensive combat operations during the war remained tied to the "movement to contact," an attrition style of maneuver that leaves the uncovering of the enemy to forward units. Tactical combat leaders use the movement to contact when they are not fed the intelligence necessary to conduct combat operations. Consequently, they are left to locate the enemy with their own resources.

The movement to contact is characterized by friendly units moving in the direction of suspected hostile forces and locating them by physical contact. This form of

12

maneuver is costly in both lives and equipment. In contrast to the movement to contact is the deliberate attack. The deliberate attack is characterized by precise, timely intelligence on the enemy's disposition. Ground combat leaders use this intelligence to plan and execute detailed operations where indirect fire support and air and naval surface fires can be coordinated in conjunction with ground maneuver to destroy the enemy. Where time prevents detailed coordination, precise intelligence fed to commanders in battle can be used to reshape the battlefield through the maneuver of friendly forces and the deployment of direct and indirect fires.

Combat experience in the Gulf War demonstrates that Marine Corps combat operations remained tied to the movement to contact. During the ground war little useful intelligence was provided to ground combat commanders. Blind to the enemy in front of them, Marine forces maneuvered forward seeking to make contact with enemy units to identify enemy strengths and dispositions. Once contact was gained and suitable intelligence acquired, ground leaders were then apprised of enemy dispositions and addressed the enemy using available combat power. The experiences of Marine Light Armored Infantry (LAI) units are particularly illustrative of this.

LAI units act as a screening force for marine ground forces, using their speed and combined arms capability to surprise and overpower forward-echelon enemy. LAI units operate in front of friendly units and provide a buffer between the enemy and the Marine main body; one of their primary missions is reconnaissance. Used as a collection tool, they uncover enemy forces as they move forward and report back intelligence on enemy dispositions and strengths. This intelligence is relayed to combat decision-makers who then deploy combat power from the main body to address the enemy threat. LAI forces

are quintessential movement to contact weapon platforms. Like the horse cavalry of the 19th century, they discover enemy through contact. Once contact is gained, they fix the enemy in place in order to buy time for follow-on friendly forces to move up and destroy the enemy.

C. INTELLIGENCE FAILURE LEADS TO IRAQI TROOPS' ESCAPE

During Desert Shield, just before the ground war started, Saddam Hussein launched a major attack designed to trigger the ground war and rout Saudi and American Marine forces defending along the Kuwaiti-Saudi border. At the time, no signs existed that the Coalition was in any hurry to invade, and Hussein's combat power was quickly eroding. Iraqi forces, pounded continuously by air, were becoming increasingly less effective as each day passed. If Hussein's forces were to crush an American attack, they needed to do it soon.

Key to the Iraqi attack was surprise. Using three front line divisions, all over 70 miles away from American and Saudi defensive positions, Iraqi commanders ordered their troops to move at night to avoid detection and devastation from American air power. There is significant evidence that Iraqi commanders may have also been aware of American satellite coverage, as they made their attack "consistent with when the satellite was not there." (Gordon and Trainor, 1995 p. 271) Their precautions were successful, and no intelligence on the impending Iraqi attack was reported to Marine forces. (Gordon and Trainor, 1995, pp. 265-270)

Fortunately the night before the attack, just as the enemy was moving into assembly positions, a Marine reconnaissance team manning an observation post on the border spotted tanks and detected a large mechanized force. The team called in air strikes,

and the following morning the smoke from the burning tanks provided ample clues as to the enemy's intentions. Nevertheless, Marine commanders dismissed the Iraqi attack as some sort of exercise and returned their attention to preparing for the future ground war. When the full Iraqi attack came just as darkness fell that same day, January 29, 1991, the Marines were still unaware of the Iraqis' plan. (Gordon and Trainor, 1995, pp. 265-275)

The battle lasted most of the night and into the early hours of the morning. As the forward traces of the enemy divisions maneuvered into the LAI screen, Marines hastily formed a defensive line to meet the advancing Iraqi attackers. At OP4, an old police post along the border, a reconnaissance team was the first to spot the forward elements of the 1st Iraqi Mechanized Division. A LAI company already operating in the vicinity rolled into the area just as the Iraqis were preparing to overrun the OP.

To save the reconnaissance team, the Company Commander ordered his LAVs forward to cover their extraction. By this time however, enemy tanks were dangerously close, and in a confused firefight a LAV was hit and destroyed by a TOW missile fired from a friendly LAV. The company commander ordered his LAVs to concentrate their 25mm cannon fire in the direction of the enemy, hoping that by doing this friendly aircraft loitering above could key in on the stream of fire and spot the advancing enemy.

Unfortunately, this did not work, and a flight of A-10's passing over fired a Maverick that slammed into another friendly LAV, destroying it in a fireball. With two vehicles destroyed, the company commander believed he was being outflanked and ordered a withdrawal to reorganize. Despite this, the Marine defense combined with close air support had been enough. After five intense hours of fighting, the Iraqi attack was stopped. (Gordon and Trainor, 1995, pp. 265-275)

Still uncertain as to what the enemy had planned, another LAI Company[1] screening just north near OP6 was hit by forward elements of the same division. This Iraqi attack began with an artillery barrage followed by illumination rounds that lit up the area as dozens of Iraqi tanks and armored personnel carriers crossed into Saudi territory and seized the OP. The reconnaissance marines escaped, but this time the Iraqi force did not continue the attack. Instead they deployed their vehicles around the position and waited for the Marines to attack.

With little idea of what was in front of him, the LAI Company Commander called in close air support while he moved within 500 feet of the OP. As the LAVs moved forward, the Iraqi mechanized force suddenly came alive and launched a hasty attack. In minutes, LAV TOW shots and close air support stopped the Iraqi assault. By morning there was nothing left but burning vehicles and surrendering Iraqi soldiers. The Iraqi's had been repulsed, and the 1st Mechanized Division retreated back into the Kuwaiti desert.

While superior Marine air and ground firepower stopped the surprise Iraqi attack, Marine units quickly learned that intelligence on Iraqi forces was severely lacking. In an effort to prevent future surprises, a stopgap measure was employed.[2] Marine OV-10s, slow flying Vietnam era propeller planes outfitted with forward looking infrared imaging devices (FLIR), were tasked to fly along the Saudi-Kuwaiti border each night and pass any enemy intelligence directly to forward combat commanders. This measure worked in the static defense that was characteristic of Desert Shield. However once the ground war began and Marine units started conducting offensive combat operations, intelligence

---

[1] As related by the Charlie Company Commander, 1st LAI Battalion, Captain Thomas R. Protzeller.
[2] Ibid.

again failed, and operations moved back into the movement to contact paradigm, as we discuss below.

Indicative of the fall back to traditional attrition warfare, the movement to contact paradigm characterized all Marine offensive combat operations during the ground war. Typically, forward combat leaders who were blind to the enemy disposition in front of them moved to contact to uncover and destroy unknown enemy units. Regarding the general weakness of this approach in the Gulf War, one example is particularly telling.[3]

On D-day, February 24, 1991, Charlie Company, 1st LAI Battalion was the screening force for Task Force Taro. Charlie Company's first objective after passing through the Iraqi barriers was the seizure of a Korean Workers Camp just 10 kilometers inside the Kuwaiti Border. As with all Marine attacks into Kuwait, Charlie Company had little information about what and how enemy forces were deployed at the camp. Given orders by the Task Force commander to reconnoiter and fix any enemy, the Company Commander moved towards the objective cautiously. Once on the objective, however, it became apparent that valuable time had been lost looking for the enemy on a position that had been abandoned weeks earlier. This prudent type of movement is characteristic of the movement to contact, for risky tactics that unnecessarily expose friendly troops can spell disaster if they are ambushed by a well-camouflaged, competent enemy. With little information on enemy dispositions, combat commanders must be cautious as they move to contact.

This very need for caution in the Marine's movement to contact operations in Kuwait can be seen as leading to the ultimate collapse of Schwarzkopf's "Hail Mary" ground campaign. That plan called for the Marines to attack first, one day before the

Army, and fix the Iraqi forces in Kuwait. This action would buy time for the Army's heavy mechanized and tank units to swing around from the west and trap fleeing Iraqis as they attempted to escape. However, the outcome of the Marine attack changed everything. (Gordon and Trainor, 1995, 265-295)

Other encounters on D-Day, similar to the one described above, quickly taught the Marines that the Iraqi defenders were not going to defend to the death as intelligence had reported earlier. It became clear to Marine Commanders that the Iraqi defense was collapsing and that their forces were fleeing back to Iraq as fast as they could. In response, Marine commanders pushed their units at breakneck speeds into Kuwait. Collapsing in the face of the Marine attack, the Iraqi forces were fleeing Kuwait much sooner than expected.

Because of poor intelligence on the enemy, the Marine and Army attacks were at that point out of sync. Realizing that the hugely successful Marine attack was violently pushing the Iraqis out of Kuwait instead of fixing them, Schwarzkopf ordered the Army to attack early. However, the Army had yet to fight the Iraqis, whom many army commanders saw as Arab equivalents of the Soviet Army, and did not have the same intelligence on the Iraqis as the Marines had. As a result, the Army "planned to fight them just as they would take on the Red Army, with massive firepower and careful coordination." (Gordon and Trainor, 1995 p. 377)

Reluctant to attack early, the Army sprung its attack at 2:30 PM on the 24th of February. The attack began with a ferocious barrage of artillery. For a half-hour, five artillery brigades fired 6,136 artillery rounds and 414 rockets at the suspected Iraqi positions on the other side of the tank and mine obstacles. The Army wasn't taking any

---

[3] Ibid.

chances; unaware that the Iraqis had abandoned many of their positions weeks before and expecting a strong defense, they threw everything they had at the defensive positions. At 3:00 PM the assault began. The Army encountered little opposition as they moved across the Iraqi defensive barriers. But it was getting dark, and progress was slow through the narrow lanes in the Iraqi obstacles. Wary of the enemy and determined to concentrate his forces, General Frank, the commander of the Army's VII Corps, suspended the attack until "every last piece of equipment had gotten through the obstacles." (Gordon and Trainor, 1995, p. 380)

In this way the main enveloping force, overly cautious because of poor intelligence on Iraqi units and unaware of the Marines' overwhelming success to the east, delayed the attack and allowed fleeing Iraqi units precious time to escape north. The next day the VII Corps movement was slow and deliberate. Each successive movement was coordinated and synchronized with artillery, tanks, and aircraft. The technique was effective; the corps met the enemy with superior firepower in every engagement. Nevertheless, the Iraqi army was fleeing north, and the few units the Corps ran into were only blocking positions established to buy time for Iraqi Republican Guard forces and other units to escape deep into Iraqi territory. By February 26, the Corps movement was so slow that Schwarzkopf personally got involved to get it moving. Earlier Baghdad had ordered a general retreat. Also, the Russians were planning to call a Security Council meeting to push for an end to hostilities. The Corps was moving too slowly, and the Iraqis were escaping to the north. Schwarzkopf knew that he had precious little time to close the back door and destroy the Republican Guard units before either they escaped or a cease-fire was called. Unfortunately, the cease-fire came too soon, and the deliberate

19

methodical movement of Frank's Corps prevented the envelopment from trapping the fleeing Iraqis.

Previously, "Schwarzkopf had left no ambiguity about the Army's mission. The Republican Guards were not to be routed, they were to be made combat ineffective." (Gordon and Trainor, 1995, p. 429) However, on March 1, after the cease-fire, American intelligence photos showed that "842 Iraqi tanks (a full quarter of Iraq tanks from southern Iraq and Kuwait) and 1,412 armored personnel carriers (half of all APC's in theater) had escaped." (Gordon and Trainor, 1995, p. 429)

What is most significant about the success of the Iraqi retreat is that the majority of the equipment and personnel that escaped north were Hussein's Republican Guard divisions. These were the divisions that were instrumental in suppressing the Shiite uprisings that occurred in the marshes in Southern Iraq following the war; these same forces were the units that deployed into Southern Iraq in 1994 to intimidate Kuwait and the UN no-fly zone. Most analysts agree that these units were pivotal in propping up Hussein's regime during the critical internal rebellions that shook both northern and southern Iraq following the war. (Gordon and Trainor, 1995, pp. 420-430)

D.   ANALYSIS OF MARINE GROUND INTELLIGENCE IN THE GULF WAR

The experiences of both Marine and Army forces in the Persian Gulf highlight what Carl Von Clausewitz described in his book, Vom Kriege (On War), as the friction of war. With little intelligence on what was in front of them, Marine units operated in the movement to contact paradigm. Once they gained an understanding of the collapsing Iraqi defenses, Marine units sped north and pushed the fleeing enemy out of Kuwait.

This threw Schwarzkopf's plan out of sync. Thus the VII Corps[4], unaware that the Iraqis were collapsing, fought a slow and methodical battle that allowed time for Iraqi combat power to escape north. In the end, the war concluded without the destruction of the Republican Guard.

Interestingly, this fog or friction existed despite the advances in surveillance and information technologies that permitted high level intelligence to see nearly everything on the Kuwaiti-Iraqi battlefield. At issue is the fact that the Central Command (CENTCOM)[5] intelligence and other high level Marine and Army intelligence (J-2, G-2) functions were designed to provide intelligence for an attrition era military. *In effect, the configuration of intelligence that had served America well in the past became irrelevant during the Gulf conflict.*

A new American military emerged during the Gulf War: a military concerned with casualties and collateral damage. The fundamental offensive doctrine had also changed; attrition warfare was replaced by maneuver warfare. As described earlier, maneuver warfare relies on superior operating tempo, surprise, and decentralized command to defeat the enemy as a system. In contrast, attrition warfare relies on a willingness to absorb attrition so that the enemy can be defeated through the systematic destruction of all its individual parts. Hence, maneuver warfare demands accountability

---

[4] The "Left Hook" or "Hail Mary" envelopment was a two Corps thrust commanded by Lt. Gen. John Yeosock commander of Army Forces in the Gulf. Lt. Gen. Frank's VII Corps was the innermost enveloping force while Lt. Gen. Gary Luck's XVIII Airborne Corps was the outermost. While this section has focused primarily on Frank's slow moving VII Corps, the reader should understand that Luck's XVIII Corps, while not similarly disposed, was also unable to close the envelopment in time to trap the fleeing Republican Guard Forces. Major General Barry McCaffrey commander of the 24th Mechanized Division (assigned to Luck's XVIII Corps) was the northern most unit in Iraq when hostilities ended. He stated "...They probably should have sent us forty-eight hours before the Marines." (Gordon and Trainor, 1995, p. 432) His Division sped across the Iraqi western desert but arrived too late to block the fleeing Republican Guards.

[5] CENTCOM or Central Command J2 is the intelligence staff that supported General Schwarzkopf during the war. As such, they were the highest echelon of military intelligence during the war.

for confronting enemy strengths when, alternatively, exploiting enemy weaknesses can save lives and collapse an enemy more effectively and efficiently.

Yet, while ground combat leaders were swiftly adopting these new operational concepts by decentralizing command and control and demanding low-level initiative from subordinates, intelligence remained tied to past practices and continued as a hierarchical, centralized organization. Thus, the flexible, high-speed analysis required to feed the intelligence demands of ground leaders during the war was an impossible task.

The Persian Gulf War may perhaps be the last twentieth century-era, conventional adversary the American military fights. Using attrition era tactics, American military power easily overwhelmed the Soviet-armed Iraqi army. Hussein's forces were no match for high-technology weapon systems like the M-1 tank, precision guided bombs and advanced tactical fighters. However, the emerging New Order Threat environment will present an entirely different threat picture for future U.S. military engagements. Operating in the movement to contact paradigm (attrition era tactics) will no longer be suitable against these threats. Conducting ground operations without intelligence on the enemy will be disastrous in this new environment. Thus a paradigm shift away from the movement to contact and towards the deliberate attack will be necessary to operate successfully in this new, emerging environment. Key to effecting this transition is the establishment of an intelligence enterprise uniquely configured to support maneuver warfare and understand and provide suitable intelligence on New Order Threats.

The Gulf War highlights the inadequacy of the present-day Marine ground intelligence organization. The challenge is to suggest an alternative configuration that is aligned with the environment to be faced in the coming century. In the next chapter, the

emerging threat environment is described. The threat environment is characterized by two major challenges: asymmetric military threats and non-conventional threats. Asymmetric military threats attempt to circumvent Western conventional superiority by developing counters to American conventional and technological dominance. Emerging non-conventional threats harness inherent organizational asymmetries to also counter American conventional dominance. Together they represent a New Order Threat environment whose complexity and asymmetric advantage will render irrelevant current intelligence practices and seriously challenge any intelligence enterprise configured expressly to meet their challenge.

III. THE CHALLENGE FOR MARINE GROUND INTELLIGENCE: MARINE CORPS ORGANIZATIONAL DESIGN

A. INTRODUCTION

Marine ground intelligence is a complex organization that was designed in the industrial age. As a result, its configuration assumed the predominate organizational form of its time: that of the machine bureaucracy.[1] As a machine bureaucracy[2] in an attrition warfare era, its design was satisfactory; however, this design is grossly inadequate to meet the intelligence demands of a new operational environment characterized by *New Order Threats* and maneuver warfare. What are the characteristics of intelligence's structural and functional design that leave it so woefully unprepared to serve 21st century Marine combat decision-makers?

This chapter describes the modern intelligence bureaucracy by first defining the fundamentals of its organization. Four elements of the intelligence bureaucracy are highlighted: 1) the centralization of power and control of resources, 2) the standardization

---

[1] The work of Arthur Stinchombe suggests that the structure of an organization reflects the age of founding of the industry. He found a relation between the era the industry was founded and its organizational design. For example, organizations of the pre-factory era - farms, construction firms, retail stores and the like- tend to rely more heavily on family personnel, retaining a kind of craft structure, whereas those of the early nineteenth century - apparel, textiles and so on - use virtually no unpaid family workers, but many clerks, a sign of a bureaucracy. Those of the next era - railroads and coal mines - tend to rely heavily on professional managers in place of owner-managers, a second stage of the developing bureaucratization of industry. (Mintzberg, 1993, pp. 123-124) Extending this theory helps explain why Marine Ground Intelligence is configured in its present design. Marine intelligence assumed the characteristics of the most prevalent organizational frame of its era: the Machine Bureaucracy.

[2] The term Machine Bureaucracy (or Machine Organization) was coined by Henry Mintzberg (Mintzberg, 1993) and is used to describe organizations that display the following design characteristics: highly specialized, routine operating tasks; very formalized procedures; a proliferation of rules; reliance on the functional basis for grouping tasks; relatively centralized power for decision making and resource control; and an elaborate administrative structure with a sharp distinction between line and staff (Mintzberg, 1993, p. 164). The reader is reminded that when the term Machine Bureaucracy is used it is referring to the Mintzberg definition rather than Weber's classical definition. Max Weber (1947) in the beginning of the 1900's developed theories on the "ideal" efficient organization. He proposed several characteristics to define this archetypal bureaucracy: division of labor, well-defined authority, formalization, and impersonal nature.

of task, 3) the focus on organizational control, and 4) the configuration of the divisional intelligence community.

Following the presentation of the current intelligence organization, this chapter provides an analysis of how the bureaucratic elements described are inherent sources of fallibility in that they limit ground intelligence's ability to adapt to the challenging threat environment and are incapable of achieving timely processing of the ever-increasing volume of information-age data. This analysis leads to the conclusion that current ground intelligence design is incompatible with the threat environment it faces in the next century.

B. BUREAUCRATIC ELEMENTS OF MARINE INTELLIGENCE

During World War II and the Cold War, warfare was essentially an industrial problem. Both sides fought with little regard for resources, raising huge armies with almost limitless masses of men and material. These conflicts of attrition warfare demanded mass forces that were effective at warfighting; thus, monolithic armies fought with each other head-on and employed every known resource to materially overwhelm their opponent.

This style of attrition warfare does not demand precise tactical intelligence for success. After all, superior numbers and technology are the key to achieving victory. Battle with the enemy was sought under almost any conditions; less important was when or where. The focus was pitting superior strength against the enemy in order to exact the greatest toll from him and force his destruction. In this context, the movement to contact was the predominate form of offensive maneuver. Tactical intelligence on forward enemy units was important in that it indicated that enemy forces were there and

movement would guarantee contact. However, detailed intelligence that indicated precise locations, weaknesses, and possible courses of action was of lesser importance, for the enemy would be destroyed not so much from military competence as from sheer force.

In an era dominated by attrition warfare and the movement to contact, battlefield intelligence could afford to move slowly. For most of the 20th century, mass armies could only fit and maneuver through certain areas, their weapons were known, and their effectiveness well understood. With both sides battling regardless of the costs, the sudden appearance of an enemy position would not greatly affect an offensive moving army. Contact was expected; men and material would be destroyed; replacements would be forthcoming.

The machine bureaucracy was an ideal organizational form for intelligence at a time when both sides were entrenched in the relatively predictable and stable task of attrition warfighting. The bureaucratic organization was thus particularly suited for an intelligence function that could be slow and deliberate, methodical, and very conventional. This is not to say that unorthodox, highly sophisticated intelligence was unknown during this period. On the contrary, great advances in intelligence were achieved, often by those working in non-bureaucratic structures. The great code breakers who aided in breaking the German and Japanese codes, code named Ultra (Rosen, 1991, p. 133), operated in unstructured and very effective organizations. These operations were pivotal in operations against the Axis powers. Nevertheless, on the whole, ground tactical intelligence was perfectly suited to a bureaucratic structure and faced little pressure to innovate and seek other organizational forms. Let us now explore the elements that define this machine bureaucracy that is Marine intelligence.

1. Centralized Organization

One of the defining elements of the machine bureaucracy is the centralization of power. In an intelligence bureaucracy this means that the majority of organizational power, decision-making authority, and resources or assets are controlled at the highest level within the organization. Typically, this is at the Marine Expeditionary Force (MEF) level.[3] Hierarchy and chain of command are tools that reinforce the vertically centralized structure of Marine ground intelligence, illustrated in the organagram in Figure (3.00).

At the top of the organization is the MEF intelligence section (G-2), the level at which all most organic assets and resources are centralized and controlled.[4] Outside intelligence agencies and collection platforms link here as well. These include national assets (e.g., satellite imagery and high level human intelligence from the CIA) and theater assets (e.g., an array of sophisticated platforms like the Joint Surveillance Target

---

[3] The MEF is the largest Marine Air Ground Task Force (MAGTF) command in the Marine Corps. The MAGTF is a unique organization that consists of a command element (CE), ground combat element (GCE), air combat element (ACE), and a combat service support element (CSSE). (For purposes of this thesis, the MEF will be studied as the MAGTF CE (highest intelligence echelon). The reader is reminded that a MAGTF CE is not limited to a MEF headquarters. In theory any tactical headquarters can be designated as a MAGTF CE.) The MEF, commanded by a Lieutenant General, is essentially a headquarters whose mission is to aid the Commanding General prosecute combat operations (i.e., the intelligence staff provides intelligence that is used for operational planning etc.) The MEF headquarters, therefore, is comprised of a large supporting staff that includes administration, intelligence, operations, logistics, and other elements. In a large contingency or war, a MAGTF is usually formed under the command of a MEF. For example, in the Gulf War, I MEF from Camp Pendleton, California, was the CE for the First and Second Marine Divisions during the ground war; I MEF was also the CE for Operation Restore Hope in Somalia.

[4] Intelligence assets are separate functional organizations that aid in fulfilling MAGTF intelligence requirements; they are categorized as organic, theater, and national assets. Organic assets belong to (are owned by) the MEF (or MAGTF CE) . Theater assets are owned by the CINC (or Commander in Chief) of a particular area of operations. Each CINC (e.g. CINCSOUTH for Latin America, CINCPAC for the Pacific, etc.) is the highest military authority in a geographic region, they oversee all military operations within their specified area. They own various intelligence assets that are used to assist in the intelligence effort in times of crises. In such a crises the MEF intelligence section would be given access to these platforms and incorporate them into the intelligence collection plan. Finally, national assets are those that are run by the various DoD and Executive agencies such as the Central Intelligence Agency (CIA), National Reconnaissance Officer (NRO) etc.

Acquisition Radar aircraft, JSTARS, that track moving vehicles and objects from high altitudes).

Below the MEF is the ground combat element (GCE) comprised of divisions, regiments, and battalions. Each division, regiment, and battalion has its own intelligence staff that supports its respective commander. The farther down the intelligence hierarchy one goes, the fewer the assets assigned. At the battalion level (S-2), only one organic asset exists: the infantry Marine.[5]

As can be seen in Figure 3.1, the MEF intelligence section is the provider of combat intelligence for the entire organization. Division, regiment, and battalion rely on

LEGEND

HUMINT - human intelligence
SIGINT - signals intelligence
TECHINT - technical intelligence
IMINT - imagery intelligence
ELINT - electronic intelligence
MASINT - measurement and signature intel
RECON - reconnaissance
SENSOR - ground sensor reporting
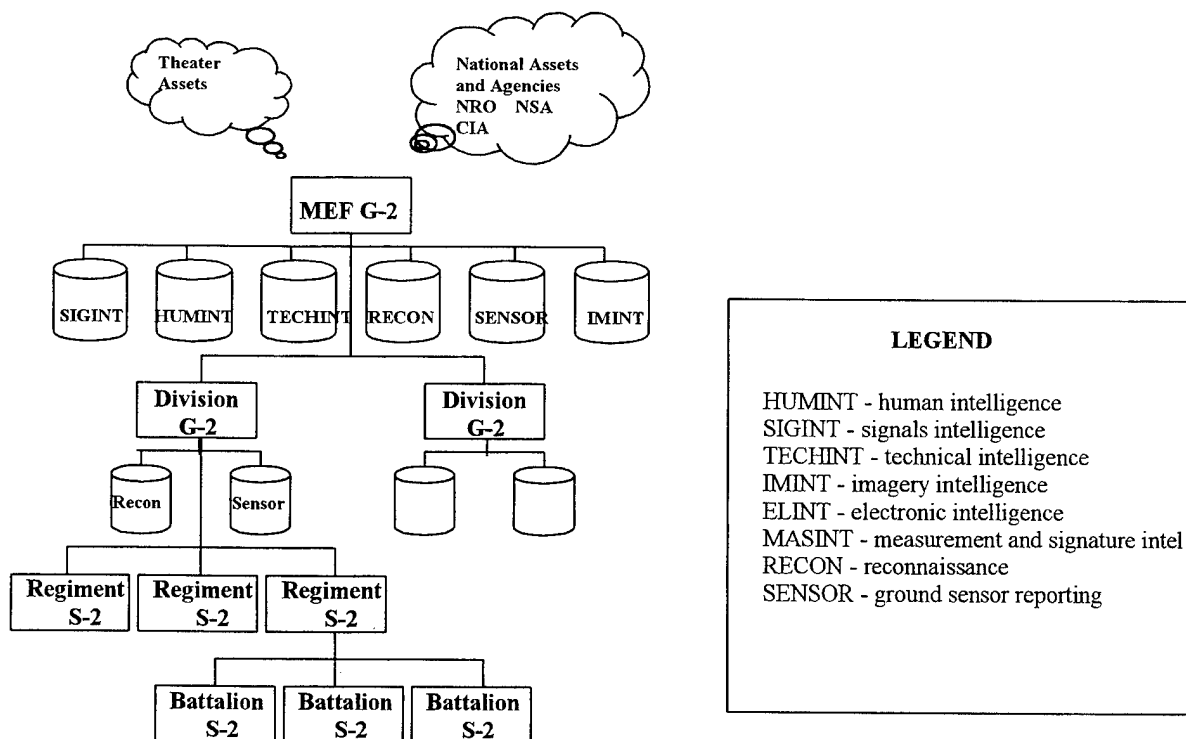
Figure 3.1. GCE Intelligence Hierarchy.

---

[5] By infantry marine the author is referring to the lack of collection assets available to the battalion. The battalion has two organic collection assets: forward-deployed marines engaged in combat and Scout Snipers who employ expert field tactics to stealthily reconnoiter enemy positions. Both these assets, however, are limited by operational reach. Because of this they are limited to collecting intelligence on

the MEF G-2 to collect, process, and analyze relevant intelligence to support their organizations' intelligence requirements.

To facilitate its operations, the MEF G-2 (or MAGTF) is organized into three sections (Figure 3.2): the Surveillance and Reconnaissance Center (SARC), the All Source Fusion Center (AFC), and the Dissemination Cell. The particular responsibilities of each of these sections are clearly delineated. The Reconnaissance Center is the reception point for all MEF organic intelligence assets; information attained here is processed and sent over the management information system (MIS) to the Fusion Center, which is the "brain" for the intelligence section. It is at the Fusion Center that organic, national, and theater intelligence is integrated to build an understanding of the enemy. This is done by comparing data from various assets to determine accuracy and by plotting valid enemy units on a situation map that forms the common enemy picture for the MEF. Fused intelligence is next sent to the Dissemination Cell where the developed enemy picture is approved by a senior level intelligence officer and forwarded to the Combat Operations Center. The enemy picture is incorporated into the MEF's situational awareness of the battlefield, and, together with his staff, the MEF commander prosecutes the war. The figure below illustrates this process and shows how the same fused intelligence is disseminated throughout the MEF to the GCE, ACE and CSSE.

enemy that are already inside the battalion battlespace. Thus, while they provide valuable intelligence, it is often too short fused to provide anything but early warning.
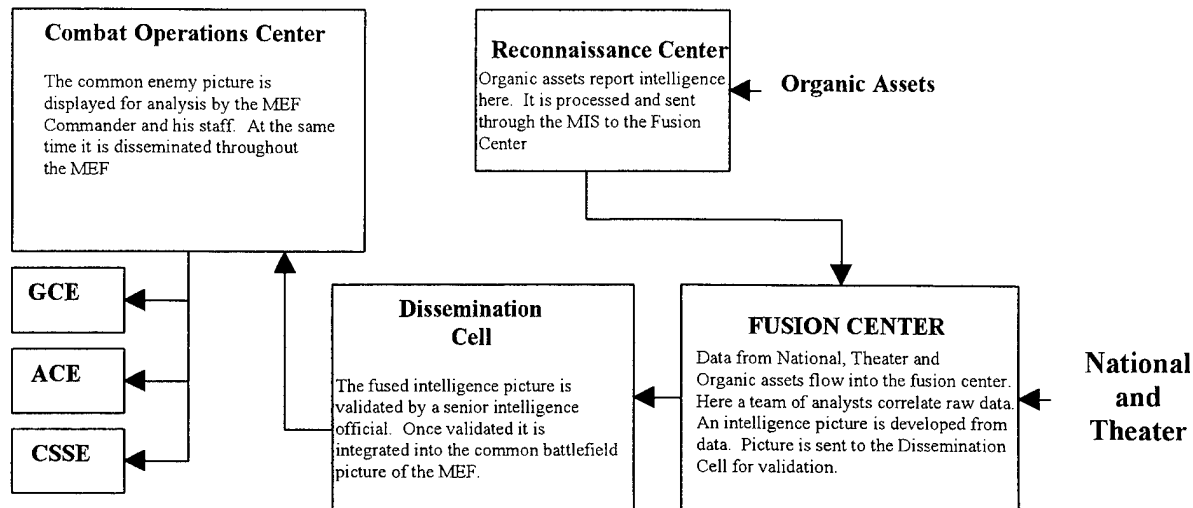
Figure 3.2. Intelligence Production: MAGTF Intelligence Cell. After (BSTF, 1997).

Because the task of intelligence is complex, it is divided up into many subtasks. The result is a division of labor that involves considerable interdependence, and therefore coordination, between specialties. The intelligence bureaucracy formally adheres to the *intelligence cycle* process to accomplish coordination of the efforts of the separate divisions involved in intelligence processing (Figure 3.3).
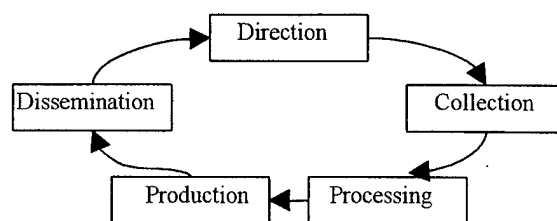
Figure 3.3. The Intelligence Cycle. After (FMFM 3-21, 1991).

The first coordinating mechanism of the intelligence cycle is the articulation of an information need. Termed *Direction*, this sets the work of intelligence in motion; direction is established by the demands of the operation. Battlefield commanders and

31

their intelligence staffs work together to identify the priority intelligence shortfalls necessary to conduct combat operations. Because they do not have the assets or connectivity to collect on these shortfalls themselves they forward their intelligence requirements to the MEF G-2 (or MAGTF), where it is prioritized with other requests. Priority intelligence requirements are then passed to the next phase, *Collection*. Collection involves the tasking and gathering of information from all available assets; it is the point where organic and non-organic agencies communicate with the MEF intelligence cell. Collection tasks these agencies and is the first to receive their data inputs. Collected data is then fed to *Processing* where it is converted into a form suitable for the production of intelligence. From Processing, the data goes to *Production* where it is converted into intelligence through evaluation, integration, and interpretation. Finally, the intelligence is disseminated back down the hierarchy to the requestor. This cycle reflects the emphasis on the efficient management of centralized resources and assets. In other words, the assembly line approach insures that the scarce resources located at the top are efficiently applied to each task. Like building a refrigerator on an assembly line, the cycle enforces a fixed, step by step, serial dependence between requestor, collector and analyst. In this way the organization can harness the benefits of specialization and division of labor, which increase efficiency and ensure the production of suitable quality intelligence. The centralized nature of Marine intelligence is therefore exemplified by the consolidation and accumulation of resources at the top of the intelligence hierarchy and by the complete dependence of lower level elements of the hierarchy on the top levels for intelligence.

2. Standardization of Task

A second element of the machine bureaucracy is the standardization of task, the breaking down of complex tasks into narrow specialized areas through the division of labor. The intent of standardization is to reduce a task into a series of simple, routine processes, thereby increasing efficiency and ensuring that every process is accomplished in the same manner. Jobs are made repetitive to require a minimum of skill and training. This results in narrowly defined jobs with routine tasks, reliance on divisions for the grouping of different tasks, and a rationalized work flow where a highly elaborate hierarchy manages coordination and communication throughout the organization. "Workers are left with little discretion, as are the supervisors, who can therefore handle very large spans of control." (Mintzberg, 1993, p. 635)

The intelligence bureaucracy seeks to simplify complex tasks so that they can be done efficiently by most any operator. Standardization ensures intelligence work is consistent and conforms to the doctrines or standards of the organization. To aid in the standardization, "recipes" or "cook book" procedures become important. Thus, when analyzing an enemy, intelligence professionals apply standardized frameworks to understand enemy actions.

Marine intelligence processes have been standardized around the two most threatening conventional enemies facing the American military: the Former Soviet Union and North Korea. Both these adversaries have been studied exhaustively and are well understood. To ensure a standard and accurate analysis of these enemies, a standardized process for analysis called "intelligence preparation of the battlefield" (IPB) was developed. This analytic method breaks down the enemy and his environment into simple blocks, facilitating comprehension of his potential actions and capabilities. IPB,

33

however, presupposes the following conditions, which will be shown in later chapters to be increasingly irrelevant in the New Order Threat environment: 1) the enemy has a doctrine, 2) that the enemy follows that doctrine, 3) we know the enemy's doctrine in detail, and 4) we have an extensive knowledge of the weather and terrain of the area of operations. (Steele, 1992)

An analyst using IPB first analyzes the enemy in order to understand his organization and how he may fight. The analyst does this by employing a set of doctrinal templates that describe the enemy's known organization and fighting methods. For instance, assume an enemy anti-aircraft site is located. Using his template the analyst could surmise that under Soviet doctrine, anti-aircraft sites usually protect important command and control nodes. Driven by this knowledge, the analyst could assign a collection asset to observe the area and look for command and control equipment like radio antennae. This formulaic approach to intelligence reduces the uncertainty associated with intelligence work and standardizes the processes so that the entire organization can achieve a certain standard level of analytic skill.

The reliance on automated systems to do intelligence work is another element of task standardization. The bureaucracy is always looking for ways to increase performance while at the same time increasing efficiency. The human element is the one part of the system that often creates the most problem. For an information processing bureaucracy, automation is an approach that can achieve both effectiveness and efficiency without having to adjust the often-unreliable human problem. Intelligence has therefore begun to pursue "sensor to shooter" designs that remove the human element altogether. Using information age sensors and MIS technologies, raw data is downloaded

34

directly from collection platforms onto a common enemy picture screen. The system

conducts its own analysis using previously designed templates. Once the system

identifies the target as enemy, available weapons engage it. This example represents the

extreme end of automated intelligence; however, such a reality is not too distant.[6] The

prevalence of task standardization in the design of Marine intelligence is clearly apparent

by the reliance on formulaic Cold War era analysis, by the use of simple processes

configured to allow standard output regardless of operator, and by the increasing

replacement of programmed system decisions for human ones.

3.   Control

Control is a third fundamental element of the bureaucracy, and it is perhaps the

most obvious element of Marine intelligence. The bureaucracy must be obsessed with

control for two reasons: tight control systems reduce task uncertainty, thereby increasing

efficiency, and organizational control reduces conflict, which typically prevails

throughout the organization. Control systems and organizational control are key

indicators of an organization more concerned with internal bureaucratic efficiency than

with supporting the consumer's demand for detailed intelligence.

---

[6] There are many within DoD that are pushing for this type of warfare. The Joint Chiefs of Staff (JCS) concept for information superiority known as Joint Vision 2010 is the most renown. It advances the development of an information sensor grid that would identify space, air, sea and ground "targets". A complete picture of the environment, and friendly and enemy forces would emerge. Called "Network Centric Warfare", this near perfect battlespace awareness would facilitate sensor to shooter warfare, where targets are identified, processed and engaged. The human element is minimal in this configuration as it slows down processing time. The key concept is increasing the speed of decision making by relying on sensor "hits" and machine processes. By so doing this "locks out" potential enemy courses of action and presents him with a dilemma he cannot overcome (Taken from a brief entitled: The Emerging Joint Strategy for Information Superiority, given at NPS in 1997).
The work of the Strategic Studies Group, a think tank that reports directly to the SECDEF, advances a similar model. Of particular interest to this work is their view on how sensor to shooter concepts will transform the way decision making and command and control is organized. They state that "...intelligence will be subsumed by operations." (Casper, 1996 p. 85) Thus, they argue that sensor to shooter technology and doctrine will require little need for an intelligence function in the future.

Designed to eliminate task uncertainty, control systems enable anyone to accomplish the task. Like a worker at McDonalds who prepares french-fries, every task is simplified and standardized. In this case, the cook places the fries on an automated device that signals the worker when finished. Little initiative is left to the worker. Control processes eliminate all possible uncertainty of task, so that the organization can operate efficiently without interruption.

The way intelligence is processed, as typified by the intelligence cycle described above, reinforces the intelligence bureaucracy's efforts to eliminate task uncertainty through standardized control processes. As described previously, the only way for a consumer to receive intelligence product is to follow an assembly line process whereby the consumer articulates the information need and submits a request for information, then waits patiently for that request to flow up the hierarchy for review, approval, processing, prioritization, further processing, and analysis, and then, finally, dissemination back down the hierarchy. Each step in the cycle has rules and regulations that govern how the task is done, ensuring accuracy and efficiency and mandating that intelligence processes be carried out to the letter. The result is that every task, every request for intelligence, is carried out in the same way.

Furthermore, the intelligence bureaucracy is not an open environment where people talk and resolve issues associated with performing a complex and ambiguous task. Rather it is configured to enforce a closed, tightly controlled system where tasks are compartmentalized and an assembly line process forces the work to be accomplished in a particular way regardless of conflicting viewpoints. Disseminated intelligence is the end product of an established, sequential effort of collection, fusion, analysis, and approval.

The intelligence cycle is conducted at the top of the organization and is performed by a small analysis cell that is overwhelmed by other similar requests. Within this configuration there is little sharing of unprocessed intelligence. Ideas from lower levels do not influence the analysis that is strictly conducted at the top level. On the contrary, the work of intelligence is reduced to a highly regimented information processing enterprise. Data is fed into the system; it is manipulated and later disseminated. Only those at the top can influence the production of disseminated intelligence. The top is therefore the provider of the corporate knowledge of the organization.

Control processes proliferate to ensure that only intelligence that has been approved by central authority is disseminated. To reinforce this, a strict hierarchy is developed, as illustrated earlier in the presentation of vertical centralization. Intelligence acquired by lower echelons is not disseminated to the corporate body until it flows up to the top and is approved. Then it flows back down to the rest of the organization. Even a dissemination authority must approve intelligence generated within the headquarters. Only after it is approved is it then disseminated.

The role of control in Marine intelligence is paramount to this machine bureaucracy. While accuracy is the goal of the hierarchical control processes, intelligence output is painstakingly slow and reflects only the opinions of the top level, which is restricted from coordination and communication with other parts of the organization.

4. Configuration of Divisional Intelligence Work

The final element of Marine intelligence's machine bureaucracy is the divisional configuration that makes up the wider intelligence community. Marine intelligence is only one piece in an enormous national intelligence bureaucracy that is driven to the

divisional form because of the diversity of the intelligence mission. Each separate

external operation or division represents the many specialty functions of modern

intelligence, such as human intelligence (HUMINT) performed by the CIA the State

Department and other agencies, signals intelligence (SIGINT) by other agencies, and

battlefield intelligence by the services and the Defense Intelligence Agency (DIA).

Each intelligence area is organized by function, to allow for the specialization of

task and the development of expertise. The functional specialties, referred to as

"stovepipes," are vertically integrated disparate operations that collect, process, and

analyze the different kinds of intelligence data for which they were designed.

Functional organization develops into occupational communities such as signals

intelligence and human intelligence; each is a separate intelligence function and has its

own career path, training program, and culture. (See Figure 3.4)
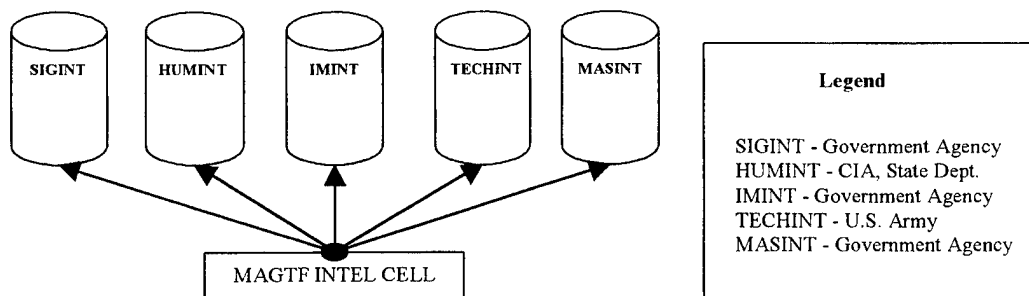
Figure 3.4. The Divisional Intelligence Community.

The combined work of each functional area is fused to build an accurate, ever-

evolving picture of an enemy. For example, to determine the position of an enemy on a

battlefield several functional areas would be tasked to collect and report information

within the realm of their expertise. Signals intelligence (SIGINT) professionals would

detect and analyze radio emissions, human intelligence (HUMINT) professionals would

interrogate local residents or captured prisoners, imagery professionals (IMINT) would analyze aerial photographs, etc. The reporting of each functional area is fused with other functional data inputs, and intelligence analysts draw conclusions as to the location of the enemy on the battlefield.

Because each division is a mini organization unto itself, there tends to be a high degree of duplication of effort across divisions. This simultaneously minimizes inter-division dependence and means that little coordination is needed to accomplish assigned tasks. As a result, lateral communication between divisions is rare. When communication is necessary, it is formal and usually follows a chain of command where it circulates up to headquarters, then down to a division, then back to headquarters, and finally back down to the sender. The need for divisional organization within the intelligence community is considered to arise from the unique expertise required in each of the various intelligence gathering realms. Divisionalization limits informal communication between divisions and creates compartmentalization of information that only slowly is able to make its way through the hierarchy to the corporate body.

C.   ANALYSIS OF MARINE INTELLIGENCE ORGANIZATIONAL DESIGN

The fundamental mission of Marine ground intelligence is to provide combat decision-makers the knowledge necessary to make informed decisions about an enemy. Designed to support attrition era warfighting, Marine intelligence assumed the most effective and efficient organizational design of the period, the machine bureaucracy.

In contrast, modern Marine Corps combat operations demand an intelligence function that can support warfare by maneuver. It must be an agile enterprise capable of harnessing the volume of information age data and generating precise intelligence on emerging new order threats.

Bureaucratic design creates a paradox of present day intelligence: intelligence work arising out of turbulent combat conditions cannot be reduced to simple bureaucratic processes or strictly hierarchical design. Nevertheless, in spite of this contradiction, military intelligence has maintained this configuration.

As the Marine Corps enters the 21st century, it is taking advantage of the information age and an ever-increasing array of powerful technologies like sophisticated sensors and information processing systems. It is also facing a threat environment that is more complex, uncertain and dangerous than that of the Cold War era. Combat leaders now demand information age intelligence to outmaneuver and counter powerful new threat operations. Confronted with a complex task, Marine intelligence requires an organizational design that can effectively manage disparate functional operations, fuse and interpret their inputs, and rapidly disseminate precise intelligence.

In the next sections of this chapter, the elements of Marine intelligence bureaucracy are analyzed with respect to these new demands of combat – and are found sorely wanting.

1.   Flaws with Centralization

The centralized-bureaucratic intelligence organization poses two major obstacles that impede its ability to fulfill its mission. It lacks the manpower necessary to process the amount of inquiry that is generated by maneuver warfare, and these few analysts are unable to appropriately respond to information age intelligence.

How does the bureaucratic intelligence cycle play out in battle? (See Figure 3.5) Assume a battalion needs to know if enemy units are located in a particular region prior to an attack. The battalion intelligence officer sets the direction, and submits his units critical intelligence shortfalls up the hierarchy. The request is processed and prioritized

and eventually sent to collections who organizes available assets to gather data on the request. Once the various assets have collected their data, the MEF (or MAGTF) collections receives the data and forwards it to the Fusion Center. The Fusion Center then processes the data into a usable intelligence product. The dissemination cell approves the intelligence product, and it is then sent down the hierarchy to the requestor. While this process may seem straightforward, in practice it is not that simple.

First, a good deal of information must be processed to coordinate the interdependent subtasks that go into filling the intelligence request from MEF. Simply requesting that an area be surveilled to determine the existence of enemy is imprecise and can lead to misunderstanding and erroneous data. To successfully exploit advanced national, theater, and organic sensors like JSTARS requires careful coordination. In most cases, system operators who are located thousands of miles from the area of operations must know precise information pertaining to the target area. Also, because face-to-face communication is often impossible due to logistical and other constraints, successfully communicating intelligence requirements is not trivial. Therefore, the MEF intelligence collections cell must coordinate carefully with all assets to ensure requests are understood.

Fusion analysis is also a complex process. Fusion intelligence analysts must have expert knowledge on the enemy. Much of the data analysts receive is contradictory and unintelligible; often it is just a series of white dots that mean nothing unless fused with other data like satellite photographs or emissions from radio broadcasts. Additionally, fusion analysts must also understand why the intelligence is needed. Will the battalion be attacking the enemy from the air or the ground? When will they attack? Understanding

information of an operational nature is critical to providing precise intelligence necessary for effectively confronting the enemy.
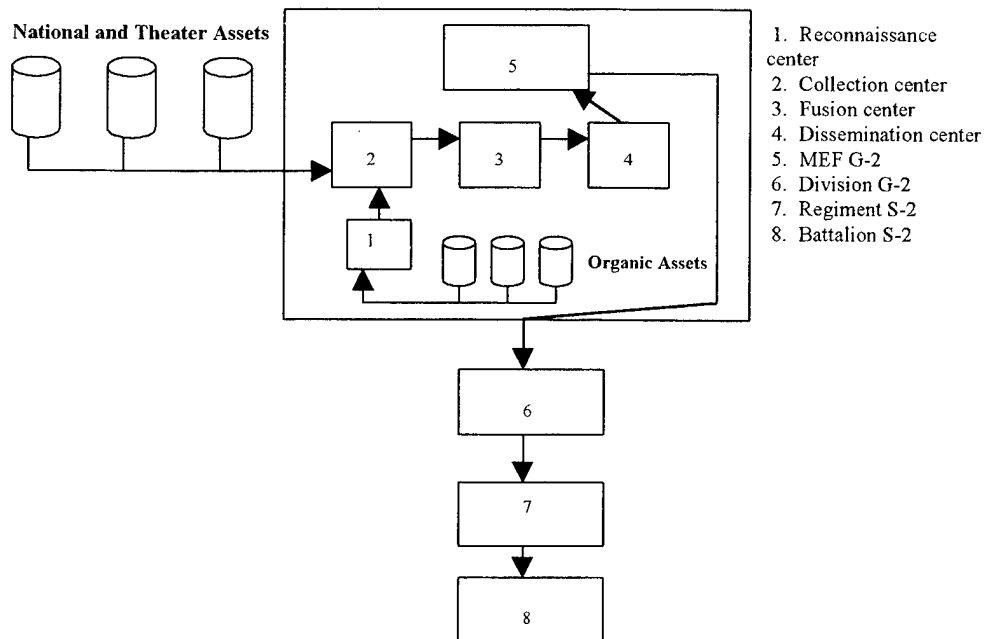
Figure 3.5. Intelligence Processing in the Intelligence Bureaucracy.

a.   Overwhelmed by Maneuver Warfare Inquiry

One obvious weakness of the centralized intelligence bureaucracy is that the greater amount of information needed to be processed, the more likely the top will be overwhelmed. For the intelligence bureaucracy, intelligence work is largely an information processing function: it collects disparate bits of data from a wide variety of sources and, through expert analysis, transforms data into intelligence. Because it is centralized and there only exists a limited number of analysts and collection experts, when the top is confronted with great numbers of intelligence requests, it quickly becomes overloaded.

The information processing scale (Driver, 1990, pp. 38-39) below (Figure 3.6) provides a graphic example of this. As the number of intelligence demands

increases, the central staff is initially able to process the requests, and the system experiences a period of positive returns to scale. As the number of requests further increases, the system reaches equilibrium. This is the point where for every one additional request the returns decrease proportionally. Called the "prohibitive region," all further demands on the centralized cell result in significant reductions in intelligence processing capability. This is where the system is unable to process data in a timely fashion, and it responds by either ignoring intelligence demands or filling them after much delay. As the MEF possess the preponderance of assets, lower combat echelons operate without intelligence.
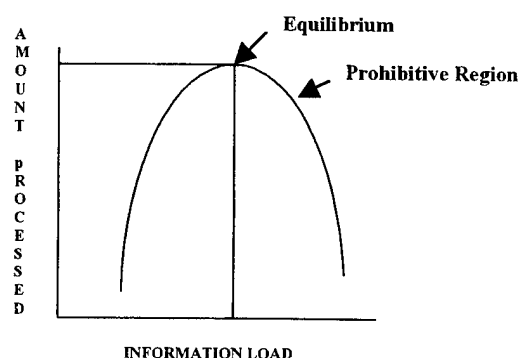
Figure 3.6. Information Processing Scale. After (Driver, 1990, p. 39)

To demonstrate this, first look at the demands of the modern battlefield. As discussed in Chapter II, maneuver warfare is now the warfighting doctrine of the Marine Corps. Maneuver warfare demands precise intelligence, for it requires the ability to circumvent enemy strengths and attack from a position of advantage. Because the identification of enemy weaknesses is not trivial, and because successful maneuver depends on the ability to identify and exploit enemy weaknesses, complex intelligence work is a key element in the successful application of maneuver warfare on the battlefield.

The task of intelligence supporting maneuver warfare is significantly different than that of supporting attrition warfare. Instead of reacting to intelligence fed from higher or lower, intelligence transforms and becomes proactive. As a result, all intelligence levels throughout the hierarchy proactively inquire into the battlespace. Each combat echelon demands a unique level of intelligence that will facilitate warfare by maneuver.

Under a centralized structure, each echelon submits requests up the hierarchy, where the majority of the assets are located. Once the requests arrive at collections, they are approved, and assets are assigned. As described previously, the data is then fused and disseminated. However, proactive inquiry demands a monumental amount of intelligence work. The Fusion Center cannot fulfill the hundreds of requests for information that accompany this level of inquiry. As a result, it quickly enters the prohibitive region and the system suffers overload.

A factor that contributes to information processing overload is that each request presents significant challenges for a small, centralized staff. Analysts are often located far from the battlespace in protected environments where they do not know or understand the complexities of the current enemy situation. When requests for intelligence are submitted, the analyst who knows little of the unique situation facing forward-deployed units must first interpret and then input them into the system. Then they must be re-communicated to the collecting asset. Both these steps introduce the probability for error and can ultimately effect the quality of the intelligence provided. Finally, once the data arrives it must be interpreted. Again, many times the fusion analysts have no idea what they are looking at, and accuracy is degraded. When

confonted with this level of inquiry, the system bogs down. Requests go unfilled or are processed and disseminated in an untimely fashion.

In the Gulf War much criticism was directed at intelligence for its inability to provide tactical commanders intelligence that was available at higher, strategic echelons. The focus of this criticism has often been directed at the dissemination technologies employed at the time. (Campen, 1992) Nevertheless, the centralized intelligence bureaucracy is not designed to provide tailored, maneuver warfare intelligence to tactical commands. The task of processing hundreds of requests simply overhwhelms the central intelligence cell. More recently, the Army confronted the same information processing dilemma as they attempted to reconfigure their organizations to adapt to the information age. That experience is worth describing here, for its lessons are equally applicable to Marine intelligence.

In March of 1997, (Brooks, 1997) the Army conducted its first exercise in a series of advanced warfighting experiments to determine the effects of information age sensors on the modern battlefield. Called Force XXI, their goal was to push sensor data to the lowest levels possible so that every soldier could have the same battlefield awareness as headquarters. With precise enemy intelligence in the hands of the corporate body, the experiment was to determine if battlefield intelligence dominance would provide friendly forces with increased lethality, increased survivability, and greater ability to control the tempo of battle. To accomplish this, a complex information management system was configured to move this common picture around the battlefield. However, while the latest information technologies were used to develop and build a state of the art MIS, intelligence remained a vertical, centralized structure. Hundreds of

45

analysts and operators, manning national, theater, and organic level assets fed an unprecedented level of data into a central fusion cell. "Every battle began with a 90 percent or higher read on the enemy... down to the individual fighting position and vehicle." (Brooks, 1997) Sensors tracked the enemy and every enemy position was located. "The enemy could not use a radio without being intercepted and located with precise coordinates." (Brooks, 1997)

As a result of this phenomenal intelligence, friendly forces were able to win the first initial contacts of every battle. However, as the fury of contact increased after initial contact, the intelligence picture began to slow. Within a very short time, friendly forces lost the near perfect picture of the enemy. While the official analysis has yet to be published, one senior intelligence officer speculated that "it had to do with the ability of the Army to assimilate the capabilities we have now." (Brooks, 1997) Referring to the centralized information processing scale, the reader can see that with a robust intelligence architecture supported with modern MIS and sensor data, the system quickly reached the prohibitive region. Once there, combat units are left on their own and are forced to move quickly into the movement-to-contact, attrition era maneuver.

b. Overwhelmed by Information Age Intelligence

A second challenge to centralized intelligence is posed by the information age data that are associated with modern 21st century sensors - data so detailed that its introduction into the centralized intelligence organization overwhelms operators and equipment alike. Indeed, the introduction of such technologies, rather than eliminating friction and the fog of war, simply confuses operators because of the overabundance of information.

To understand this, consider the following: modern sensors provide narrow bands of data that, shown graphically, contribute to the situational awareness of a battlespace. To add meaning to the displays, analysts require multiple inputs from assets to validate "hits." These hits are often represented in the form of white dots and can represent many things besides actual enemy vehicles. However, white dots fused with an understanding of the enemy and validated by other collection assets can contribute to a highly accurate battlespace picture.

Again, this process is not trivial. Operators must have an appreciation of what is on the battlefield. Whereas this is not a difficult thing for forward-deployed units that live and fight on the battlefield to do, it is extremely difficult for a centralized intelligence bureaucracy, where analysts are far removed from the battlefield and their appreciation and understanding of the environment is greatly reduced. Therefore, white dots may indicate T-72 tanks in the attack to a scope-centric operator, but may indicate something entirely different to an intelligence professional who is fighting on a battlefield cluttered with metallic debris. These complications are multiplied as an over tasked and overwhelmed Fusion cell attempts to fill the intelligence demands of a multitude of different users.

2.   **Flaws of Standardization**

It took forty years for the Army to develop doctrinal templates on the Soviet and North Korean armies. How do you develop a template against an adversary that cannot be easily identified because it does not move in large formations or use large pieces of military hardware? Applying standardized formulas to intelligence work will surely prove unreliable against the new threats emerging in the next century.

The following chapters show that networked and asymmetric adversaries seem do not seem to require a set pattern. Without an encyclopedic data array that describes the enemy in detail, modern intelligence practices will be greatly strained. Therefore without prepared, in-depth knowledge of the cultural, political, economic, geographic and military attributes of New Order Threats, formulaic analysis models like IPB will be rendered irrelevant. Left without an analytic approach to understand these threats, intelligence professionals will be severely challenged.

Furthermore, the context of military intelligence is not simple and stable; rather, it is chaotic and turbulent. Intelligence work arising out of turbulent combat conditions cannot be reduced to simple tasks, the processes cannot be made repetitive, and so standardization is impossible. In the emerging environment, threats are increasingly less centralized and regimented. Former Soviet and North Korean templates no longer provide answers on how an enemy will fight. Indeed, emerging threats think on their own, and they adapt quickly to American technology. To counter these smart adversaries simple, formulaic intelligence processes will prove unreliable and even misleading.

An additional weakness in the area of standardization of task relates to the nature of information technologies, which tend to lure operators into a sense of passivity and complacency. Operators become monitor-centric, only reacting when the system picks up targets. In this circumstance, there is a tendency to believe the technology and accept whatever it indicates. If the system says there is nothing, there is nothing. However, the nature of New Order Threats presents serious problems for system-centric approaches. These threats will be less visible to sophisticated intelligence systems and will operate across a highly disordered, dispersed, nonlinear battlefield. Intelligence professionals

who are accustomed to operating where systems reveal everything, are unlikely to detect New Order Threat operations. As a result enemy operations may go undetected and thus harness tremendous battlefield advantage.

3.   Flaws of Control

It is readily apparent that the context of military intelligence cannot be reduced to an assembly line process where a few analysts at the top produce the corporate enemy picture with little input from within the hierarchy. Intelligence must be the sum of the total organizational understanding towards its environment. The many bureaucratic control processes designed to reduce task uncertainty and conflict restrict formal and informal communications within the hierarchy. This in turn isolates the top from the rich knowledge that abounds at the lowest levels of the organization.

While control measures are well suited for tasks that are simple and routine, intelligence work is neither of these things; it is complex and dynamic. When confronted with a rapidly changing threat picture, control processes restrict organizational adaptation. They block the individual and group innovation necessary for successful adaptation. Instead of encouraging organization-wide discussion and analysis, the bureaucracy handles such non-routine actions by formalizing them and bumping them up the hierarchy where they often are diffused and even lost before they reach the top of the structure.

The inability to adapt to a changing task is particularly evident when the intelligence bureaucracy confronts *New Order Threats*. As discussed below, New Order Threats quickly adapt to intelligence technology and analytical techniques. When they do so, they change the entire calculus for threat analysis. Intelligence production must

change and adapt to New Order Threat intelligence counters or they will operate without detection. The following example is illustrative of this point.

In a recent exercise[7], intelligence dominance was quickly achieved over an aggressive and unconventional enemy. Using an array of sophisticated sensors and a team of analysts, friendly intelligence had a complete track on every enemy unit on the battlefield. By day two, however, after approximately seven hours of combat, the enemy began to maneuver differently on the battlefield. Where before, he would aggressively move tanks and other vehicles around the battlespace in an effort to out-flank and gain access to friendly rear areas, by day two his tactics changed. He maneuvered less. In fact, unless uncovered by forward moving friendly forces, he would not move at all. When he did maneuver he used densely vegetated approaches that had thick overhead canopy. He avoided moving his forces in convoy, preferring instead single vehicle deployments and operations. Finally, he relied more heavily on scouts and the light infantry battle.

To the intelligence section glued to sensor outputs and compartmentalized from forward fighting units, the battlefield appeared empty. Nothing moved. As a result, the official read from headquarters was that the enemy was not on the battlefield, and an enemy free picture was disseminated throughout the organization. However, what the

---

[7] During September of 1997, the 4th Light Armored Reconnaissance Battalion (minus, reinforced) conducted exercises to support an advanced concept development managed by the ASCIET program at the National Guard Training Center, Camp Shelby, Mississippi. The program's objective was to operationally test the Grenadier Brat (tactical IFF system) in near combat conditions. To support the exercise a robust intelligence capability was attached to the LAR battalion to determine if battlefield intelligence dominance would provide friendly forces, (a LAV company), with increased lethality, increased survivability, and greater ability to control the tempo of battle. The unit selected as the OPFOR -- a platoon from the National Training Center, Fort Irwin, CA was equipped with Former Soviet weapons (T-72, BRDM, BMP, ZSU-23-4, etc) and operated using a mixture of classic Former Soviet centralized tactics and non-standard, American tactics.

compartmentalized bureaucracy did not understand was that the enemy had adapted. After taking a beating from friendly maneuver and fire, the enemy learned that unnecessary exposure to overhead sensors almost always resulted in assured destruction. Therefore, the enemy began to operate in manner that exposed him less to these sensors. Unknown to higher headquarters, forward friendly units were engaging enemy forces operating vehicles along unmarked and highly vegetated trails in the training area. Also, as contact was gained with the enemy, single vehicle battle positions were uncovered, well camouflaged and uniquely positioned to avoid detection from aerial sensors. In less than seven hours the enemy had countered friendly intelligence and developed an asymmetric battlefield response that left friendly maneuver units with no intelligence on the enemy to their front. Forced to operate in the attritionist, movement-to-contact paradigm, the company suffered its highest number of friendly casualties, seven vehicles destroyed.

Because these asymmetric developments remained at the lower levels of the hierarchy, restricted due to bureaucratic control measures, the top was unaware of their development and therefore unable to quickly adapt. Eventually, the intelligence cell was able to learn of the enemy counters, but only after detailed debriefs had been conducted. Battlefield debriefs are formal communication devices that are conducted to capture battlefield events. They flow up the hierarchy in a methodical manner and reach the top where they are often ignored because an already overwhelmed intelligence staff does not have time to read them.

In this exercise a robust intelligence staff supported one maneuver unit. It took one day to process the battlefield debrief and organize a counter to the enemy's

51

asymmetric innovation. In combat, an intelligence staff of equal size would support

dozens of different maneuver elements fighting across a varied battlespace. Limited to

formal communication and coordination measures in a tightly controlled bureaucracy,

recognizing, and then countering an enemy asymmetry would take much longer. Such

delay would afford the enemy significant battlefield advantage.

4.   Flaws of Divisionalization

Marine intelligence and the wider intelligence community struggle with several

problems associated with the divisional configuration. First, the nature of the divisional

bureaucracy precludes lateral communications between divisions. This often creates

tunnel vision, causing workers to see only the task involved within the scope of their

division. As a result, work is often duplicated between divisions, wasting valuable

resources and time. This also prevents effective collaboration between experts found

within separate divisions. Therefore the stovepipe configuration tends to

compartmentalize valuable information, hiding it from the corporate body. Information

that could be useful for one division's operations is sealed within the confines of another

division. Only after the top processes it, is it circulated. By then, the information is often

outdated and useless.

A second reason stovepipe divisions are an inappropriate design is that they are ill

suited for the level of agility necessary to match New Order Threat operations, which

demand great organizational agility and flexibility. Stovepipe divisions must be able to

quickly identify enemy evolution and quickly adapt to it. However, within the divisional

form, information often is unavailable to the entire organization until it circulates to the

top. Divisions may be unaware of enemy evolution and fail to adapt. Friendly forces that

are left operating with intelligence practices that have been countered by the enemy could lead to disaster.

By its nature, the divisional form is a slow and tedious approach to intelligence work. The duplication of work, the compartmentalization of valuable information, and the barriers to lateral communication waste valuable resources and slow intelligence production. In an era where military leaders demand information age intelligence to conduct warfare by maneuver, intelligence must be quickly available.

D.   SUMMARY

Table 3.1 provides a summary of the elements of the Marine intelligence bureaucracy and the implications of remaining in the current configuration in the coming century. This chapter has illustrated the fact that, by design, bureaucracies do not process complex information fast. They operate best in simple and stable environments and have trouble assessing phenomena that have not been previously understood and documented. They are centralized and quickly become overwhelmed by increased information demands.

Elements of the Intelligence Bureaucracy	Challenges for Intelligence	Implications
Centralized	-Centers resources at the top of intelligence hierarchy. -Low level elements dependent on top for intelligence.	-Top quickly overwhelmed by information load; little intelligence produced.
Standardization of Task	-Uses formulaic Cold War era analysis. -Designs intelligence as series of simple processes configured to allow standard output regardless of operator. -Relies on systems instead of people.	-Not configured to analyze complexities of New Order Threats. -New Order Threat environment demands a different kind of intelligence work. - New Order Threats more difficult to track using information age sensors.
Control	-Reduces intelligence into hierarchical process where output is slow and reflects the opinions of the top. -Mandates accuracy through control process; output is slow and represents opinion of disconnected top. -Restricts coordination and communication within the organization.	-Process is slow and hierarchical, not suited for New Order Threat environment. -Process is unable to adapt to asymmetries characterized by New Order Threat operations.
Divisionalization	-Limits informal communications, creates tunnel vision and impedes interdivisional collaboration. -Information often compartmentalized in separate divisions, not available to corporate body until circulated through hierarchy. -Slow and tedious approach to intelligence.	-Process is slow and hierarchical, not suited for New Order Threat environment. - Less likely to adapt to asymmetries characterized by New Order Threat operations.

Table 3.1. Summary of the Marine Intelligence Bureaucracy.

The standardized, information-processing approach to intelligence, characteristic

of the intelligence bureaucracy, reduces the complexities of analysis into rote, formulaic

processes that are limited to regimented, well-studied, conventional adversaries.

Divisionalization and strict reliance on formal communications compartmentalizes

information, often hiding it from the corporate body. Duplication of effort is often the result. Collaboration between divisions is limited, so analysis is often division centric. This produces distorted analysis that is often unable to identify complex, evolving threats.

The intelligence bureaucracy's demand for control restricts informal communication within the hierarchy. Information that flows up the formal hierarchy is massive and complex, and as a result much of it is cut and reduced to prevent overload. Even when understanding a predictable enemy, central authority often becomes overwhelmed and is therefore consumed in just understanding what is going on. Consequently, valuable intelligence remains at the higher echelons of command and usually never makes it down to tactical units.

When confronted with unpredictable *New Order Threats* that display non-linear attributes, bureaucratic intelligence is completely outclassed and may not even detect, much less identify and analyze them. Designed for an adversary that is predictable and that can be broken down into pieces and understood with linear logic, the intelligence bureaucracy is unable to apply its strengths of efficiency and formalization to threats that are not easily understood.

Furthermore, maneuver warfare places overwhelming demands on the intelligence bureaucracy. Proactive inquiry floods the central intelligence cell with demands for information age intelligence, overloading the system and reducing its processing capability still further. With all the tools for collecting intelligence at the top, lower echelons are left without intelligence. As a result, tactical units do not receive intelligence when they require it, forcing them into attritionist tactics.

The weaknesses of the intelligence bureaucracy highlight a fundamental principle of 21st century ground intelligence. *Intellect is the cornerstone to successful ground intelligence work.* Perhaps in a previous age, when threats mirrored the Soviet model and clung to regimented tactics, centralized processes and sophisticated sensors could provide the answers. However, the coming chapters argue emerging threats are increasingly less centralized and regimented. They think on their own, and they adapt quickly.

To counter these smart adversaries, Marine intelligence will need to look vastly different from the way it does now. It must be organized around and designed to enhance the deployment of intellect. Information systems aid in the collection of information and the delivery of intellect, but they are not intellect unto themselves. Intelligence professionals must harness intellect by freely and proactively inquiring into the battlespace and by receiving directly critical battlefield information in a timely fashion. Attrition era intelligence practices and organization must be abandoned if intellect and its deployment are to shape future Marine operations. In sum, Marine intelligence must be designed to be an intellect-centric, knowledge based enterprise. Configured with the right tools, organized around intellect and its deployment, Marine operations demand an intelligence function that can support warfare by maneuver. After exploring in the next few chapters the nature of emerging threats, this thesis will be in a position to describe just how such an enterprise could be configured.

IV. THE ASYMMETRIC MILITARY THREAT

A.   THE CHANGING THREAT PICTURE

"What is the foremost future security threat facing the United States in the twenty-first century?" Many intelligence estimates answer this question with the following response: "conventional, cross border aggression." Two significant policy-setting studies reinforce this view. The 1997 Quadrennial Defense Review describes large-scale, cross border conventional threats as the leading challenge to the United States, stating that "more than one aspiring regional power will have both the desire and the means to challenge U.S. interests militarily between now and 2015." The National Defense University's 1997 Threat Assessment adds that, "in the next decade, the highest prospect for an intense military confrontation is the outbreak of conventional conflict between regional powers." Other leading military and civilian positions reiterate these forecasts.[1]

However, in contradiction to such assessments, an analysis of the present day environment reflects a far different reality. Cross border, conventional wars represent less than 3% of the 37 different conflicts waged during the last seven years. Furthermore, declines in world military spending, force strengths, and foreign weapon acquisitions also shed serious doubt on this prediction. While the end of the Cold War may explain much of this decline, the fact remains that major cross border, conventional conflict has become

---

[1] While most government and non-government threat assessments are now recognizing low intensity conflict (LIC) as the predominant form of modern warfare much of their analysis is still tied to looking for Cold War era cross border, conventional aggression. Please see the Heritage Foundation's "Restoring American Leadership" (Holmes, 1996) Indeed the way the American armed forces is deployed and currently configured clearly demonstrates that conventional-cross border conflict is considered the predominant military threat facing this nation.

increasingly less likely for several reasons. First, belligerent nations are reluctant to confront each other militarily because the economic and political costs have simply become too high. Additionally, the clear conventional superiority displayed by the United States and the West during the Gulf War has seriously undermined the confidence of potential aggressors to risk confronting American technology and firepower.

Within this context a new form of warfare may be emerging. Cognizant of American conventional might, aggressive twenty-first century threats will most likely avoid military operations that are vulnerable to American technology and tactics. Instead, such threats may be developing new operational forms that seek to operate beyond American military dominance. Those tactics may include the capability to execute rapid, undetectable operations that achieve victory not limited to immediate tactical success. Under a new asymmetric form of war, success may be measured in terms of *access* and *favorable opinion* across the political, social, and economic spectrum.

Consequently, this chapter proposes that the application of asymmetry to counter Western and American conventional power is central to this new style of war.. Shedding monolithic, Cold War era conventions, these new asymmetric militaries will rely on lean, agile forces equipped with fewer, high cost, high-technology weapons. The emergence of these new militaries may be the first sign of an asymmetric response to American conventional and technological dominance.

The importance of knowing one's enemy was recognized over 2500 years ago by the Chinese general and author, Sun Tzu. He wrote, "If you know the enemy and know yourself, you need not fear the result of a hundred battles." Applying Sun Tzu's

philosophy to understand how future conventional enemies will contend with American power offers valuable clues into what the battlefield of the future may look like. Accordingly, this chapter presents data that suggests the framework for twenty-first century inter-state warfare may assume new characteristics in avoidance of American conventional war dominance. The movement towards asymmetric fighting is one of the foremost characteristics of this transformation. Pushed to seek asymmetry to confront American military power, the data reveal that several nations are redesigning and fielding new forces that are likely to challenge American conventional power. Adopting leaner, more agile formations and deploying decentralized, potently armed forces, these new militaries may pose serious threats to future Marine Corps operations.

This chapter first defines the environment that is inhibiting conventional warfare and compelling asymmetric innovation within non-western militaries. Data is presented to illustrate probable asymmetry efforts in several nations. The chapter then describes the nature of these doctrinal and technological counters to American power. After laying the statistical groundwork to support this chapter's hypothesis regarding asymmetric military transformation, a case study on the modern day transformation of China's military is analyzed in light of this argument.

Noting the massive reforms the Peoples Liberation Army (PLA) is undergoing to demonstrate China's military transition from a monolith to an increasingly more powerful and agile force, this study identifies several asymmetric developments appearing within China's vast military. To illustrate the nature and power of China's evolving asymmetric military, an analysis of a Chinese attack on Taiwan will follow. Juxtaposed against the modern Taiwanese and American militaries, the clear advantages of China's new,

asymmetric military will underscore the changing nature of twenty-first century conventional conflict.

B.   FORCES COMPELLING AN ASYMMETRIC RESPONSE

The build-up of conventional weapons and forces, hallmark of the Cold War, is no longer the pattern of the day for enemies seeking military advantage over Western forces. In fact, a fairly straightforward review of recent events illustrates how major-armed conflicts are inhibited by the very superiority of Western, especially American, conventional forces.

Throughout the Gulf War, the United States demonstrated clear conventional war dominance. The remarkable success of American technology and combat power displayed during that war sent chilling signals to the world's great military powers. In less than 100 hours of ground combat, it was clear to the world that twentieth century, conventional warfare had been rendered virtually obsolete. Any nation that dares to confront the West must fear invincible weapon systems, hailstorms of precision guided munitions, and assured destruction of its military power. Additionally, recent events in Iraq, Iran, and North Korea reveal that direct confrontation with the West also can result in disastrous economic consequences. Whether physically blockaded or sanctioned by an international coalition, economic ruin of the challenger is almost always inevitable. Consequently, direct confrontation with the West has become an unappealing alternative and a no win-situation.

The precedent in international relations, established after the Cold War, is to aggressively contain major-armed conflicts. A formal, predictable sequence of globally agreed upon activities are taken to bring disputes to resolution. First, heavy international pressure is applied. Next, economic and military sanctions are levied. Where necessary,

60

UN forces are deployed to separate the belligerents and to enforce no fire zones. Because of the unified worldwide response, hostile military aggression is therefore a difficult and costly pursuit. Beyond the international pressures, the additional potential for direct American and Western military intervention and the associated cost factors increase the risk of direct conventional conflict by orders of magnitude. These factors help explain why major-armed conflict has declined as a means of settling disputes.

Nevertheless, international relations historically have been marked by military conflict spurred on by nationalism and ideology. If the future resembles the past, then the twenty-first century world environment will be no different in this respect. In fact, as a growing number of nations, particularly in Asia, continue to expand economically, they can be expected to become more aggressive as they seek to influence and control their surrounding environment (MCIA, 1994, p. 2). Such nations may look to accomplish this by using military power. It is likely, therefore, that nationalism and ideology will continue to fuel future military actions and bring about direct military contact between belligerent or rogue governments and the United States.

1.   The Nature of Modern Day Conflict

While nationalism has sparked conventional, cross border aggression in the past and may continue to do so in the next century, the recent past suggests an interesting anomaly to this pattern: since the end of the Cold War, major-armed conflict[2] has declined by over a third (SIPRI, 1996). Out of an average of 35 conflicts, 97% were _intra-state_. Only two were inter-state: the Gulf War (1991) and the India/Pakistan border

---

[2] Major-Armed conflict as defined by SIPRI are conflicts that produce over 1000 casualties.

disputes (1993-to present). Every intra-state conflict was low- intensity in nature.[3] The reasons for conflict varied; however, for analysis they are divided into disputes over government (G) or territory (T). On average, 53% were disputes over territory with sub-state actors attempting to separate from a central government. The other 47% were typically incumbent governments facing non-government opposition. (See Table 4.1)

Region	1990		1991		1992		1993		1994		1995		1996	
	G	T	G	T	G	T	G	T	G	T	G	T	G	T
Africa	8	3	8	3	6	1	6	1	6	1	5	1		
Asia	5	10	3	9	5	9	4	7	4	7	4	8		
America	5	-	4	-	3	-	3	-	3	-	3	-		
Europe	-	1	-	2	-	4	-	6	-	5	-	3		
Middle East	1	4	2	5	2	3	2	4	2	4	2	4		
Total	19	18	17	19	16	17	15	18	15	17	14	16		
Total	37		36		33		33		32		30		27	

Table 4.1. Major-Armed Conflicts. After (SIPRI, 1996).

These numbers are significant and indicate a clear trend as humanity enters the twenty-first century. While conventional war accounts for less than three percent of the total number of conflicts waged during the last seven years, low-intensity warfare has now become the predominant form of armed conflict. Should this trend continue over time, it would suggest a decreasing likelihood of major conventional war between nation-states and an increasing likelihood of smaller, less defined LIC conflicts.

---

[3] Low-intensity conflict (LIC) can be distinguished from conventional conflicts in some important respects (Ware, 1990). 1) They result more from conditions of widespread socioeconomic and political unrest than from issues of national sovereignty; they therefore manifest the revolutionary redefinition of the political order and culture (Ware, 1990). Accordingly they may take on regional or global political and ideological dimensions. As a consequence, they can occur in the transnational arena, that is, without political boundaries. LIC protagonists oppose regimes that have established political and military institutions. LIC protagonists do not have such power and seek to destroy it. 2) Finally LICs are protracted; the choice of weapons, strategy, tactics and employment of forces is asymmetrical; and the insurgents disregard conventional notions of warfighting. (Ware, 1990)

Additionally, this data suggests that the world's powerful nation-states are entering a period of interwar peace. Since the close of the Cold War an interim period of relative inter-state peace and stability seems to have begun, threats are uncertain and nations scramble to prepare for the next conflict. The present interwar period may have begun roughly around the close of the Gulf War in 1991. SIPRI's data clearly indicate that, since that conflict, inter-state, major-armed conflict has nearly disappeared.

To many theorists, the current interwar period is not unlike the interregnum between WWI and WWII (Millet, 1994). During that period, defense resources of the great powers like the United States and Western Europe were limited but technological advances and corresponding changes in operational concepts occurred steadily. That era witnessed the development of carrier aviation, armored blitzkrieg, amphibious doctrine, air defense, and strategic bombing - all innovations that proved to be pivotal forces in the ensuing war. Simply stated, militaries that failed to innovate and harness the new developments of the period were simply outclassed and quickly defeated by those who had done so. The French, British, Norwegian, Polish, and Soviet army contacts with German blitzkrieg tactics during the first part of WWII are prime examples of this point. (Van Riper, 1997)

A parallel entry into another interwar epoch may have commenced with the West's victory over Communism. The West, with a proven and highly potent military capability lead by U.S. military power, and with victory firmly in hand upon the close of the Cold War, possesses clear military dominance. Accordingly, potential rival nations may be using this period to reorganize and prepare for future confrontations. If this is the case, the greatest concern is that these nations may use the sophisticated, expensive

advances achieved by the West to quickly leap frog into new generations of technology.

Avoiding the prohibitive development costs of first generation interwar developments[4],

they may leverage the savings to develop the next generation of weapons and doctrines.

In the following section, changes in global military infrastructure are explored and found

to highlight potential "interwar" transformations now occurring in several non-western

militaries.

2.   Global Military Downsizing

To investigate the recent changing nature of military forces, it is essential to first

determine how military spending, military force size, and foreign weapon acquisitions

have changed worldwide since 1985.[5] SIPRI and IISS data are the sources of information

presented in the following tables, with total world defense spending shown in table 4.2;

military force size shown in table 4.3; and foreign military acquisitions shown in table

4.4.

1985	1994	1995
1,173,441	821,578	814,481
31% decline from 1985 to 1995		

**Table 4.2. Global Defense Expenditures, 1985, 1994, 1995
(US$m, CY95$). After (IISS, 1996).**

1985	1995
27,131.9	22,533.2
17% decrease from 1985 to 1995	

**Table 4.3. Global Numbers in Armed Forces, 1985, 1995
(In millions). After (IISS, 1996).**

---

[4] The advances currently being exploited by the Revolution in Military Affairs are considered to be the first generation of interwar developments.   They include technologies like stealth, information and sensor technologies, etc.
[5] 1985 is used as a beginning year for this analysis because it reflects the height in Cold War spending and military force structure.

1987	1995
80,069	30,230
62% decrease from 1987 to 1995	

Table 4.4. Global Numbers of International Arms Deliveries, 1987, 1995. After (IISS, 1996).

Much of the significance of this data can be explained by the world peace "dividend" that occurred following the collapse of the Soviet Union. Three key points can be extrapolated from these data. Each is important and cannot be explained solely by the closure of the Cold War. First, there is a substantial and continuing decline in global defense expenditures between 1985 and 1995 (31%). Much of this statistic is explained by the downsizing following the Cold War. Nevertheless, underlying this world-wide trend is a surge in the procurement of advanced weapons. According to IISS there has been a major demand for advanced weapons since the Gulf War among many non-western nations (IISS, 1997). This increased demand accounts for a larger and larger share of global defense expenditures. This may indicate a global trend away from large quantities of less sophisticated and cheaper platforms to fewer, more high-tech, expensive ones. According to IISS, large-scale procurement of tanks and other conventional weapons has been reduced in favor of fewer, more powerful, similar systems.[6] Second, there is an equally significant and continuing decline in the size of these same armed forces (17% decrease). Discharging the hordes of personnel required to man twentieth century era conventional armies, many militaries are shedding excess labor and building

---

[6] An example of this is in the numbers of Main Battle Tanks (MBTs) and fighter aircraft being purchased by many less developed nations (Egypt, Iran, Saudi Arabia, China, India, Pakistan, Taiwan, etc.) Many of these nations are procuring fewer MBTs and fighter aircraft but are acquiring the best systems money can buy (IISS, 1996). The most popular tanks on the international weapons market are the Abrams M1 tank and the most advanced versions of the Former Soviet T-72 and T-80. The same is true for advanced fighters (F-16 and MIG-29). The reasons for this revolve around economics and strategy. These nations are making concerted efforts at acquiring and maintaining modern twenty-first century forces. Accordingly, they are shedding attritionist mentalities (overwhelm adversary with hordes of men and material) and seeking

smaller, highly professional forces. Finally, international arms deliveries have shrunk significantly from 1987 to 1995 (62%). Consequently, the numbers of tanks, fighter aircraft, and other warfighting equipment that usually constitute the international arms exchange has declined significantly.

The big picture painted by these three declining aspects of armed forces across the globe is that many nations appear to be transitioning from Cold War era militaries that were equipment and labor intensive to new, twenty-first century militaries that are lighter and require fewer men and material.

3.   Non-Western Conventional Military Transformation

While the end of the Cold War explains much of the decline in world military infrastructure, two additional trends serve to highlight the conclusions advanced previously. First, a block of economically advancing nations is *increasing* defense spending as a result of sustained rates of high economic growth. Second, this same block of economically advancing nations is, for the most part, reducing the total size of and significantly altering the structure of their armed forces (See Table 4.5).

Country	GDP Growth	Restructuring of military?	Defense Expenditures 1994 US$m,CY95	Defense Expenditures 1995 (%Chg) US$m,CY95	Force Size 1985 (000)	Force Size 1995 (%Chg) (000)
Iran	Increasing	Yes	2,340	2,460 (+5%	305	513 (+68%)
Egypt	Increasing	Yes	2,234	2,417 (+8%	445	436 (-2%)
India	Increasing	Yes	7,638	8,289 (+9%	1,260	1,145 (-9%)
China	Increasing	Yes	28,945	31,731 (+10%	3,900	2,930 (-25%)
Indonesia	Increasing	Yes	2,486	2,751 (+11%	278.1	274.5 (-1%)
Malaysia	Increasing	Yes	3,142	3,514 (+12%	110	114.5 (+4%)
Singapore	Increasing	Yes	3,118	3,970 (+27%	55.0	53.9 (-2%)
Taiwan	Increasing	Yes	11,457	13,136 (+15%	444	376 (-15%)

**Table 4.5. Economically Advancing Nations and Military Transformation.
After (IISS, 1997).**

---

advanced weapons and technology to adapt to information age warfighting that emerged from the Gulf War. (IISS, 1997)

These data provide small clues that help demonstrate how a number of nations may have begun to equip and organize their militaries differently. While precise conclusions cannot be drawn without an in-depth analysis of the military reforms occurring within these nations, the shedding of forces and the increasing expenditures on defense reveal highly probable military transformations. Reducing force strength while simultaneously increasing defense spending may indicate the incorporation of new military technologies and doctrines.

Many of these militaries for whom data is shown were armed and trained by the Former Soviet Union. As a result, Soviet doctrine and tactics predominated within these establishments: they were highly centralized, regimented, mass armies. Their large numbers of cheap, reliable tanks and artillery compensated for their lack of sophisticated weaponry. These militaries were attrition style forces, designed to fight and win through overwhelming superiority of numbers and equipment. Accordingly, they demanded large quantities of personnel and equipment to function.

In contrast, the information presented here demonstrates a possible shift from Soviet style organization to one of a possible new, as of yet undetermined typology. What is certain is that these nations have cast off significant numbers of personnel and are acquiring large quantities of Western, hi-technology weapon systems and equipment. All these signals may indicate a gradual transformation from Soviet like formations to more modern, agile ones.

C.   THE POSSIBLE NATURE OF THE ASYMMETRIC RESPONSE

American conventional dominance can be structured into four broad categories. First, it has the capability to project power across the globe. Second, once it has amassed

its forces it can bring to bear overwhelming firepower. Third, it possesses state of the art technology and weapon systems. Finally, it has powerful intelligence systems that can see and identify significant military weapons and formations.

Each of these four categories presents serious challenges to potential adversaries. However, what has propelled American military power to the forefront of military dominance is its leading edge in what is currently being described as the Revolution in Military Affairs. Central to the RMA and American dominance is the successful development and incorporation of precision guided weapons, advanced sensors, unmanned aerial observables, and sophisticated information systems. Successfully used together in the Gulf War and improved upon in the seven years since, these are the technologies and operational concepts that provide the clear conventional dominance the American military presently enjoys.

However, military history is replete with examples of adaptation. For every innovative development there often follows a more powerful response or counter. Bronze and iron as offensive instruments of war replaced stone weapons. The chaotic tactics of the German hordes overwhelmed the Roman legion. The organized armies of Europe were transformed by weaponry like the cannon, cartridge, machinegun, poisonous gas, barbed wire, the tank, and the airplane. The great defensive tactics and barriers that developed during World War I were rendered irrelevant by German blitzkrieg tactics of WWII. The aircraft carrier replaced the battleship. Equally likely are future military developments that will counter present day American conventional dominance.

American conventional dominance presents potential adversaries with strong incentives to pursue asymmetric warfare to assure military success, to minimize losses,

and to protect vital economies. To operate successfully against American conventional dominance, future aggressor nations may frame military operations to operate outside of American conventional strengths. To counter high-technology sensors, precision weapons, or maneuver warfare, future aggressors may embrace new military practices which incorporate rapid high speed offensives, strong defenses to deter conventional response, undetectable forces and the enlistment of emerging, non-conventional threats[7] to support conventional actions.

Identifying possible counters to American conventional dominance such as these is important, as it provides key insights into how future adversaries may engage American military forces (See Table 4.6). Several potential areas where asymmetric responses are likely to emerge include counters to the very four factors that currently account for U.S. superiority: precision weaponry, maneuver warfare, advanced sensors, sophisticated information processing, and conventional dominance. (Stavridis, 1997)

---

[7] Please see Chapter V for a complete analysis of emerging, non-conventional threats.

Factor Contributing to American Conventional Dominance	Asymmetric Response
Precision Weapons	Hardening Burying Dispersing Multiplying Confusing
Maneuver Warfare	Responsive Warfare
Advanced Sensors	Blinding Dispersing Multiplying Burying Confusing
Sophisticated Information Systems	Overwhelming Underwhelming Attacking
Conventional Dominance Worldwide response Well trained and equipped forces	Rapid intervention Cheap, crude missiles Weapons of Mass Destruction Nonlinear warfare

Table 4.6. Asymmetric Conventional Responses. After (Stavridis, 1997).

1. Precision Guided Weapons

An enemy confronted with precision weaponry would design a defensive strategy to ensure the survivability of its forces. The fundamental tenet of an effective defensive strategy is to avoid detection: what cannot be seen cannot be targeted, and what potentially can be seen must be *hardened*. Hence, defensive techniques would include the construction of hardened, underground sites to protect critical command and control nodes. The *dispersing* of military assets throughout a region to complicate collection and targeting would be another fundamental tactic. Examples would include the deployment of assets within urban areas and no-fire areas such as hospitals, schools, and other civilian

sectors. Such actions would also present targeting and collection difficulties. The key to countering precision weaponry is *confusing* American intelligence through rapid mobility and the use of deception and camouflage. (Stavridis, 1997)

As an example of such asymmetric responses to precision guided weapons, Saddam Hussein during the Gulf War effectively protected and employed his SCUD launchers by using rapid mobility, simple camouflage, and decentralized tactics. Hussein's SCUD threat was one of the primary intelligence and targeting priorities of the war. The effort to locate Hussein's SCUD systems consumed precious overflight time of billion-dollar intelligence and required the attention of special forces commandos. In the end Schwarzkof's CENTCOM staff was unable to ever find more than a handful of these dreaded terrorist missiles that rained on both Israel and Coalition forces. The Coalition's inability to target and knock out Hussein's SCUDS gives testimony to the extreme effectiveness of simple techniques in foiling precision systems.

In the future, techniques such as mobility, dispersion, and decentralization coupled with new evolving technologies will place even greater demands on collection and targeting efforts. Current developments like stealth and other new deception technologies will proliferate as they become cheaper and more accessible. The deployment of these asymmetric responses to American military dominance can be expected within a few short years, and their successful incorporation will significantly enhance the effort to counter precision weaponry. (Stavridis, 1997)

2.   Maneuver Warfare

Maneuver warfare is one of the central organizing tenets of the Revolution in Military Affairs (RMA) (Stavridis, 1997). It was developed during World War II within the German Army and is now the doctrinal warfighting concept of the United States

Marine Corps. Maneuver warfare treats the enemy as a system of interrelated parts working together to achieve a particular mission. It focuses on the destruction of the operating dynamic of the system rather than the destruction of all its component parts. Fundamental to this concept is that attacking the operating dynamic will cause the system to collapse and cease to exist as a cohesive entity. It is at this point when the enemy is presented with a rapidly deteriorating situation it can not understand or react to that the enemy is outmaneuvered and defeated. A counter to maneuver warfare may exist within its very nature as a rapid, offensive oriented operational style. Called *"responsive maneuver"* it combines static defenses with rapid counterattacks that attempt to outflank, isolate, encircle and then destroy decentralized maneuvering units (Stavridis, 1997). New, fast moving armored vehicles combined with smart, precision guided missiles may provide the equipment necessary to conduct such operations. (Stavridis, 1997)

3. Advanced Sensors

The sophisticated array of modern sensors that are designed to identify movement, communications emissions, and other critical intelligence present potential adversaries with a formidable operational problem. Innovations of the American RMA allow for near real time sensor to shooter capabilities. Hence what can be seen can be destroyed. To avoid detection future enemies will move their operations from terrain that can be easily surveyed by collection platforms to cluttered areas where identification and tracking is nearly impossible (*dispersing, burying, multiplying*). Such areas include urban environments, jungles, forests, mountainous areas etc. In addition an enemy might use anti-satellite systems, dazzlers or lasers against optics and powerful jamming and anti jamming technologies (**blinding**). Another technique is to overwhelm sensors with clutter or other devices to prevent accurate assessment (**confusing**). Deception and the

72

use of stealth and other rapidly advancing technologies may also be employed to prevent

effective intelligence collection. (Stavridis, 1997)

4. Sophisticated Information Systems

The ability to fuse information from the myriad of intelligence platforms and

widely dispersed friendly units is another hallmark of the American RMA. At no other

time in history have systems been developed that allow for a complete picture of friendly

and enemy positions to be displayed in near real time. This common operational picture,

when perfected early in the next century, will provide American military forces an

unprecedented advantage on the battlefield.

Countering this capability may take several forms. First, an enemy may learn to

trick the system by *overwhelming* or *underwhelming* it. Advanced information

technologies tend to lure operators into a sense of confidence. Operators come to expect

that the system will provide them the only "true" picture of what is happening. Thus,

when white dots on a computer monitor are not present, there is nothing to worry about:

there is no enemy. When successfully spoofed, information technologies and their

associated sensors do not inform decision-makers with critical intelligence; rather, they

lull them into a sense of over-confidence. Attacking the information system is another

counter. Whether an enemy deliberately targets critical command and control nodes,

jams essential communication channels, or employs effective information warfare tactics

against C2 nodes, the disruption for any length of time could be disastrous. American

tactics rely on coordinated fire support, intelligence and logistic support. These agencies

are often not co-located with the warfighter, and disruption of information could

dangerously expose deployed tactical units to enemy actions.

5.   Conventional Dominance

American and Western forces can bring to bear tremendous combat power to every corner of the globe within a relatively short period of time. Employing precision weaponry, maneuver warfare, advanced sensors, and sophisticated information systems, well-trained, highly professional service members possess significant battlefield advantages over other conventional militaries. To operate successfully against American conventional power, future enemies may look to new technologies and tactics that exploit American weaknesses. One concern is that future adversaries may seek new equipment and doctrines that generate *rapid, high-speed* operations. Used effectively, a potential enemy could launch an attack and secure objectives well before an effective military response could be initiated. Another concern is the potential use of *cheap, crude missiles and mines*. The enemy's massing of low cost but highly accurate cruise missiles against targets could pose serious problems for deployed American forces. Even Aegis, Patriot and Star Wars anti-missile systems could be quickly depleted of anti-missile weapons if faced with a massive missile attack. Equally problematic are mines. Saddam Hussein effectively denied an amphibious assault from the sea because of the massive flooding of mines in the littoral region surrounding Kuwait and Iraq. Mines are a significant challenge and while they can be removed, the process is time consuming.

Another counter to conventional dominance is the potential use of *weapons of mass destruction* (WMD). Such devices may range from low yield tactical devices to highly advanced chemical and biological weapons. Their employment must not be assumed to be constrained because of American nuclear weaponry. Indeed, as WMD technologies improve, it is possible that their employment may not even be recognized

74

until their full effects have been unleashed. Worse, identifying who employed the device may be difficult, as third party terrorists may be used to insert and detonate such devices. Until accurate identification can be determined, reciprocity is confused. Once identification is ascertained, the world community may impose serious constraints on how reciprocity will be inflicted.

Other counters include those that go beyond what can be imagined presently. Such discoveries and innovations that could completely change the way war is fought and won are the most dangerous. These types of development are not impossible. The accelerated advances in electronics, computing, and other high-technology areas within the last few decades indicate more than ever that the twenty-first century promises to be an age where technology and operational concepts will transform much faster than any other time in history. Areas such as *non-linear dynamics* and chaos and complexity may be understood and employed successfully in war. Rapid incorporation and successful employment of new paradigms and technologies could provide future adversaries dominance out of proportion to their political, economic, and military strength. (Stavridis, 1997)

D.   CHINESE PLA CASE STUDY

The ongoing transformation of the Chinese People's Liberation Army (PLA) is a perfect example of the nature of non-Western asymmetric military response to Western conventional military dominance. The PLA military transformation highlights two asymmetric developments designed to enhance successful power projection. First, recognizing the vulnerability of massed troops and equipment to Western intelligence collection and targeting, a reorganization of sectors of the army has begun. With a focus on power projection and survivability, China is transforming its army from large Soviet

75

style formations to smaller airborne and marine forces.[8] Second, recognizing its inability to outperform Western air power, China has invested in a low tech, inexpensive asymmetric response: the missile. (SIPRI, 1995, pp. 359-389)

Let's begin with a discussion of China's move to enhance power projection. In 1984 the Deng Administration officially recognized that China had no major peer threat and that major war was not likely for the foreseeable future (at least 50 years); (SIPRI, 1995, p. 362). As a result of this assessment, the Chinese military underwent a series of major cuts. In ten years, total forces were reduced by one million, spending as a percent of GDP was cut from 10% to 7.5%, the Ministry of National Defense (MND) was reorganized and downsized, and thousands of facilities were turned over to the civilian sector. The political leadership in China changed the national priority from the military to the economy, stating that a modern military would arise out of economic success in the industrial sector.

At the same time (1984-1994) China entered a new phase as a military power in Asia. Shifting its focus from deterrence of foreign aggression to power projection, China began to build a military that could provide a credible presence throughout the region. It used the downsizing to realign and transition its military to fit with this new mission. Two crisis areas serve to further motivate Chinese movement into power projection. First is the conflict over the oil rich region known as the Spratley Islands. China, Vietnam, the Philippines, and Malaysia all have claims in this region. Significant to China is that the Spratley Islands are estimated to possess 2 trillion dollars worth of oil reserves. As China

---

[8] Information regarding the PLA's transformation of its Army and specifically its airborne and marine corps units can be found in SIPRI's 1995 Yearbook. Several FBIS articles also contributed including "Chinese Armed Forces Increase Sea-Crossing Offensive Capabilities", Wide Angle, 16 July 1997, by Liu Hsiao-chun.

faces increasing energy challenges in the 21st century due to its modernization efforts, the Spratley Islands are seen as critical to the continued growth of the Chinese economy. The second crisis area is the dispute over Taiwan. China has unequivocally stated that it will use force if Taiwan declares independence, develops nuclear weapons, slides into chaos, or forms military alliances. China has seemed content, in the past, at the pace of talks with Taiwan and the progress thus far made. However, recent incidents like the election of the nation's first democratic President and the strong overtures at declaring independence have lead to serious confrontations.

These two crises have served to crystallize power projection as the predominant military mission for the Chinese armed forces. As recently as 1990 major military realignments have occurred that further demonstrate China's dedication to this mission. The People's Liberation Army Air Force (PLA) has deployed its forces on China's eastern and southern coasts. At the same time, PLA is consciously moving from "a posture appropriate for coastal defense to one of sea control over the extent of its territorial claims and Exclusive Economic Zone" (SIPRI, 1995, p. 380). Other indications like the expansion of paratroop capabilities and marine infantry in the PLA serve to further support the evidence for this apparent military restructuring.

Another aspect of China's military transformation involves the attempt to develop and produce advanced weapon systems like the Su-27 fighter aircraft. It is uncertain whether they are capable of leaping from second generation aircraft to advanced fourth generation aircraft so easily. Though past experience clearly demonstrates that acquiring and producing advanced active control (fly by wire) aircraft was beyond their technological capability, China has not given up. China's careful approach to defense

modernization may enable it to bypass an entire generation of development, rapidly

incorporating new technologies and doctrines 20 years from now just as their economy

mushrooms. (Pillsbury, 1993)

Apart from the restructuring effort aimed at power projection, China seems to be

dedicating the majority of its resources to missile development. Aware that it is

incapable of deploying high performance aircraft to counter Western air forces, the MND

appears to be developing highly accurate missiles as an asymmetric response. Chinese

missile designers reportedly use the U.S. Global Positioning System (GPS) for pre-launch

and mid course correction. Missiles of this variety were launched into the China Sea

during the Taiwan confrontation in early 1996. The great advantage to such weapons is

that no nation in the world possesses a system that can adequately destroy incoming

missiles. The Patriot counter missile system is probably the best such system in the

world, yet it only has an estimated 20% kill ratio. Inexpensive and easy to produce,

China could mass hundreds of such missiles against a land or sea target and no known

platform, space or ground, could counter it.

By strategically placing hundreds of missile batteries along its coast, China could

deny American naval forces entry into the region. Unable to deploy from aircraft carriers

and with few air bases in the region American airforces would be hard pressed to

generate enough sorties to neutralize the missile threat.

Missile development and the restructuring of the PLA represent two possible

asymmetric responses to American conventional dominance. The following scenario

demonstrates how these two asymmetric developments may be employed to foil World

and American intervention and guarantee Chinese military and political victory.

E.   PLA ATTACK ON TAIWAN

To illustrate the potential effectiveness of China's asymmetric developments against conventional American military forces, this section speculates about a hypothetical PLA attack on Taiwan.

The major obstacles currently deterring a PLA attack against Taiwan are the Taiwanese army and the American lead reactionary force that would shortly follow any Chinese military attack. Similar to the reactionary force deployed during the Taiwan crises in 1996, an American task force could include two full carrier battle groups with thousands of marines and several hundred fighter aircraft. Chinese military leaders have expressed considerable concern about the technologies used by the US against Iraq, as well as anxiety over the poor performance of their own technologies and similar Soviet equipment in the hands of the Iraqis. Consequently, a Chinese attack against Taiwan would be designed to avoid direct American military confrontation.

An American military response revolves around power projection, the massing of overwhelming firepower, state of the art weapon systems, and powerful intelligence platforms that give indications and warnings to alert and frame military action and strategy.

To militarily overwhelm Taiwan, the PLA would need to execute a lightning fast assault that would neutralize the Taiwanese military and secure the island before an American Task Force could respond. Once Taiwan is successfully in Chinese hands, any American military response would be severely constrained because of the likelihood of precipitating a nuclear exchange. Thus, a successful Chinese attack would need to meet these three requirements: immediately destroy the Taiwanese military, quickly secure the

island, and deploy a missile engagement ring around the region to prevent American or other forces from responding.

Each of these tasks involves significant asymmetric transformations in military technology and doctrine, demanding avoidance of the enemy's strengths and exploitation of his vulnerabilities. In this case the PLA generates two distinct military responses to Western conventional dominance: a reliance on missiles and the development of light, highly mobile shock troops. Both these developments operate outside Western conventional dominance. They are unique developments that have no effective western peer. By deploying missiles, the PLA exploits a significant Western defensive vulnerability. Unable to provide a suitable defense, American forces would be forced to operate outside the missiles effective range. Furthermore, missiles are easy to conceal and difficult to track; they are perfect weapons of surprise. Taiwanese forces, unaware of Chinese missile power, could be overwhelmed and annihilated by a surprise missile attack. Light, highly mobile shock troops are also easy to conceal and are perfect surprise forces. Highly trained and operating under the element of surprise, they could overwhelm a sleeping conventional force unprepared for an attack.

Using these asymmetric forces together, the PLA would destroy the Taiwanese military, secure the island, and prevent an American military response. A possible scenario might play out in this way:

China launches an attack on major Taiwanese airfields, military sites, and other significant facilities[9] using precision missiles. Simultaneously several paratroop brigades are airlifted and dropped on Taiwan with the mission of destroying all remaining

---

[9] Taiwan only has one major port its destruction in an initial attack would seriously impede rapid force closure from American forces stationed in Japan.

Taiwanese military forces. Within 24 hours, Taiwan could be in PLA hands. Caught by surprise, America would not have time to put adequate forces in theater. Assuming a 96 hour response time, American forces would move into the theater of operations just when Chinese forces were putting the final touches on fully incorporating Taiwan into the PRC.

American conventional forces would be powerless to prevent such a takeover and even less capable of deploying enough forces to retake the island. Given the fact that China has nuclear intercontinental ballistic missile capability, it can be assumed that their use would be threatened if an effort were made to retake Taiwan. American and world response would be limited to international outcry and potential economic sanctions. However, because of the negative effect this would have on the world economy, it is doubtful that sanctions would be long lasting.[10]

F.   SUMMARY

This case study demonstrates how a lesser conventional power could and may transform and seek asymmetric operations to confront and out maneuver American conventional dominance. Using asymmetry as a fighting principle, nations such as China, Iran, India, Pakistan, Iraq, Russia, and others are transforming their militaries and acquiring powerful capabilities. The proliferation of nuclear, biological, and chemical weapons underscores this.[11] The increasing number of transfers of advanced

---

[10] The dive in the stock market during the first weeks in November of 1997 demonstrate how moderate instability in Asian markets can have significant effects on the U.S. and World economies. A major confrontation with China would create orders of magnitude greater chaos.

[11] Dr. David Kay, formerly chief UNSCOM inspector in Iraq and now with SAIC, recently gave a talk on new threats to U.S. security at the National Defense University early in 1997. His comments centered on proliferation issues. Some facts he highlighted included: 1) General Anatol Kuznechev, the senior Russian official who was head of the latest nerve gas program, was incarcerated for over a year for smuggling nerve gas technology to the Syrians. He was instrumental in helping the Syrians establish a never gas program. 2) A Korean native was arrested in Japan in April of 1996 for shipping sarin precursor to North Korea. Police reported that this had been a long-running operation, and there was a substantial amount, perhaps in the tons, that had been previously shipped. 3) Early in 1997 a Russian official admitted that in November of 1993 two drunken Russian workers managed to steal two complete Russian tactical nukes from a factory

technologies like inertial and GPS navigation systems, computer information systems, and satellite surveillance systems also highlights this point. Furthermore, as demonstrated by the PLA example, other non-Western militaries may also be realigning their conventional forces to operate successfully against the high-technology, conventional superiority of twenty-first century Western forces. Shedding highly regimented, centralized organizations and pursuing leaner more agile force structures, these militaries will seek to get inside Western decision cycles, enabling significant advantage over them.

Using asymmetric options like missile technology and light, rapid deployment forces, these asymmetric conventional adversaries severely challenge the capabilities of the bureaucratic Marine ground intelligence enterprise. Asymmetric military threats out think and out maneuver an enterprise designed to accommodate simple and predictable adversaries. Unable to track and monitor their actions because they are hard to identify and understand, intelligence is placed in a quandary and left unable to understand threat actions. Left undetected or misunderstood these threats exercise powerful battlefield advantages that afford them great operational capabilities. These powerful military threats will exploit these battlefield advantages and seek to defeat Marine forces asymmetrically. Once engaged in conflict, asymmetric tactics may focus on producing casualties and destroying equipment. In an age where US casualties are unacceptable, future asymmetric conventional adversaries will have many advantages.

---

in the Urals. The warheads were later captured and returned. 4) A Soviet submarine launched guided missile and ERSHA navigation sets were found in Iraq three years after the Gulf War by international inspectors. Of very late Soviet design, the equipment had inertial navigation technology that was capable of being reversed engineered and applied to Iraqi WMD delivery platforms. 5) Recent media reporting have highlighted the role of China as a major smuggler of WMD and advanced technologies to rogue nations like Libya, Iraq, Iran and North Korea. Most agree that any advanced technology entering China is quickly redistributed to anywhere in the world willing to pay for it.

The next chapter presents an analysis of another powerful New Order Threat that promises to present grave challenges to Marine operating forces and render Marine ground intelligence practices increasingly less effective and relevant. Called emerging, non-conventional threats, these threats, like asymmetric military threats, also harness asymmetry to overcome American conventional dominance. They are quick to adapt, difficult to detect and nearly impossible to destroy through conventional means. Again because of their unique nature, Marine ground intelligence practices are severely challenged when confronted with these threat actors.

V. EMERGING NON-CONVENTIONAL THREATS

A.   IS HISTORY REPEATING ITSELF?

Centuries ago, criminal bands organized to control society's political and
economic systems. Led by the most ruthless of individuals, these bands flourished and
dominated the Medieval Ages and many other periods of recorded human history. Often
outnumbered and technologically inferior to the civilizations they preyed upon, these
gangs or hordes had miniscule resources and were forced to innovate or face defeat.
Catalyzed by their inability to face the Roman Legion or Medieval Knight on equal
terms, they evolved and crafted new forms of warmaking. With little more than the skins
on their backs and simple weapons, these warlords and bandits devised tactics that
focused on exploiting the weaknesses of their enemy, allowing them significant strategic
advantage in spite of their rudimentary, low technology weapons.

The opposite tack was taken by "civilized" forces. Certain in their belief that they
could defeat any potential adversary, particularly the rabble of German hordes or
marauding criminals, modern militaries were slow to adapt to the new warfare of their
challengers. Rome fought a protracted war with the innumerable German hordes using
tactics that had long been rendered obsolete. The battlefield that the hordes brought to
history was too chaotic, bloody, and thoroughly disorganized for the traditional Roman
Legion. The Knights of the medieval period faced similar extinction because of an
inability to adapt to the new threat of their time. Encumbered by expensive, heavy armor,
the knights (high tech for *their* time) faced a quick demise when the rabble of warring

gangs innovated and developed low technology infantry to stop the horse and bludgeon the Knight with sticks and stones.

History may be repeating itself. Many of the "new" threat forms emerging from the chaos of the Cold War are employing these centuries old tactics and principles to great advantage against the conventional military powers of our time. Though now equipped with modern weapons and hard-earned insights into conventional military vulnerability, this emerging class of non-conventional threats displays characteristics similar to those of ancient and medieval era warfare and may be undergoing transformations in response to American conventional and technological dominance.

The goal of this chapter is to define and highlight the emergence of this new breed of threat as well as to articulate the severe challenges they present to Marine ground intelligence. Accordingly, after an overview of this new class of threats, this chapter traces their early evolution and describes their nature, unique typologies, and powerful ability to adapt to their environment. Termed low intensity or non-conventional, these threats are shown to resemble traditional Cold War era, low intensity conflict (LIC) with the added features of guerrilla warfare. Having their origins in the developing world, these threats will be shown to be operating now in modern societies.

Once the foundation for understanding emerging, non-conventional threats has been laid, this chapter explores and reviews cases of how society's response to these threats drives them into new designs and tactics. An analysis of the strategies being used by these threat organizations to adapt and shift their focus from the defeat of modern militaries to the defeat of the political, economic, and social will of the nation-state is presented. The chapter concludes with an analysis of the evolution to network design,

leaving no doubt that these threats are powerful and present great challenges to Marine ground intelligence practices and design.

B.   EVIDENCE OF GLOBAL INSTABILITY

As the United States enters the next millenium, it faces an uncertain world environment.   Now more than ever, the power and number of potential threats cannot be easily predicted or classified. It is in this environment that the United States will most likely face two major threats: asymmetric military threats and emerging, non-conventional threats.

Previously in Chapter IV, global military trends data were used to illustrate how lesser conventional powers could and may transform to seek asymmetric advantage to counter American conventional dominance. The analysis in that chapter highlighted several potential areas where asymmetric transformations could evolve to counter American precision weaponry, maneuver warfare, advanced sensors, sophisticated information processing, and conventional dominance.

Additionally, figures for recent conflicts (SIPRI and IISS data) were used to demonstrate that there has been a steady decline in the number of major-armed conflicts[1] since the end of the Cold War. That data clearly indicated that cross border, conventional war has fallen to its lowest level in modern history, while intra-state, low intensity warfare has risen to become the predominant form of war. [2]

Given the declining number of major armed conflicts, it would be expected that world order, overall, would have experienced a period of stabilization. On the contrary,

---

[1] As defined by SIPRI and IISS data, Major Armed Conflicts are those in which the number of victims is greater than 1000. Please see SIPRI data presented in Chap. 4. Major Armed Conflict represents both inter and intra state conflict.
[2] Represents less than 3% of total armed conflicts.

several key indicators reveal that the reduction in major-armed conflicts has *not* been accompanied by a corresponding decrease in worldwide chaos and disorder.

To track the degree of global internal civil conflict and strife, let us analyze refugee and internal displacement statistics (see Tables 5.1 and 5.2). Internal displacement is a direct reflection of the impact of wars and civil strife on civilians within a nation; the effects of natural disasters do not contribute to its numbers. Refugee data, unlike internal displacement data, does not solely measure the impact of wars and civil strife; it represents the numbers of people fleeing their towns and villages in any emergency situation.[3] Including the refugee statistic as an indicator of internal disorder is valid here for two reasons: it highlights the chaos caused by natural and unnatural events, and it may indicate that the environment is ripe for or already plagued by non-conventional threat exploitation.

A review of the data for migrations of refugees fleeing internal conflict and for internally displaced people shows that these figures have not declined significantly over the period from 1990-1995, and have even in a few cases risen. In broad terms, large numbers of refugees fleeing a nation's border, or large numbers of internally displaced people, can be assumed to indicate varying degrees of regional chaos and disorder. As the number of worldwide major-armed conflicts decline, it would be expected that both these statistics would also decrease by some order of magnitude. Yet, over this period (1990-1995) internal displacement declined by only 1% and refugee numbers by 8%. This small decline does not match the 30% decrease in major-armed conflict over this same period.

---

[3] Natural disasters such as earthquakes, high winds, flooding, etc., contribute significantly to refugee statistics. Despite this, the refugee statistic is a valid indicator of internal disorder. Natural disasters are often the catalyst for non-conventional threat operations. Witness Somalia, Ethiopia and other Western African nations.

In fact, the numbers of internally displaced people rose dramatically from 1990 through 1994 and has only recently declined. Given the reduced conflict, it is reasonable to expect a much greater decline in world chaos as reflected by these two indicators.

REGION	1990	1991	1992	1993	1994	1995
Africa	5,451,150	4,531,950	4,650,342	6,119,800	5,879,700	5,222,300
Europe	737,600	675,200	3,157,500	2,858,900	2,421,500	2,520,700
Latin America	171,950	131,500	109,700	101,650	297,300	256,400
East Asia and Pacific	600,100	974,700	684,700	487,600	444,100	452,850
Middle East	5,698,600	6,850,700	6,370,850	4,825,900	5,447,750	5,449,100
South and Central Asia	4,098,600	4,061,050	2,341,700	2,151,400	1,776,450	1,386,300
World Total	16,758,000	17,225,150	17,314,792	16,545,250	16,266,800	15,337,650

Table 5.1. World Refugee Migrations by Region. After (IFRC, 1995, 1997).

REGION	1990	1991	1992	1993	1994	1995
Africa	13,504,000	14,722,000	17,395,000	16,890,000	15,730,000	10,185,000
America	1,126,000	1,471,000	1,304,000	1,700,000	1,400,000	1,280,000
Asia	4,325,000	4,865,000	4,009,000	3,545,000	2,388,000	2,155,000
Europe	268,000	825,000	1,596,000	2,765,000	5,195,000	5,080,000
Middle East	1,290,000	1,480,000	830,000	1,960,000	1,710,000	1,700,000
World Totals	20,513,000	23,363,000	25,134,000	26,860,000	26,423,000	20,400,000

Table 5.2. Internally Displaced People by Region. After (IFRC, 1995, 1997).

An important point surfaces when internal displacement data is analyzed in conjunction with SIPRI major-armed conflict data. What is evident in the summary chart below (see Table 5.3) is that the number of countries experiencing internal displacement far surpasses the countries experiencing major-armed conflict. In fact, there are twice as many nations experiencing internal displacement problems as there are facing major-

89

armed conflict.[4] Equally revealing is the comparison between major-armed conflict and refugee data. It is apparent from this analysis that the number of countries experiencing movement of refugee populations outnumbers those experiencing major-armed conflict by nearly three to one.[5] Such information is enlightening as it reflects to some degree the potential for LIC involvement in internal disorder and chaos in many nations.

Nature of Instability	Number of Nations Affected
Major-Armed Conflict	25
Internal Displacement	46
Cross-Border Refugee Problems	66

Table 5.3. Comparison of Major-Armed Conflict with Chaos Indicators.

The data presented here highlight a paradox that is beginning to define the twenty-first century threat environment: major-armed conflict may no longer be the predominant cause of regional chaos and disorder. What then is creating the unexplained levels of instability if major-armed conflict is not the primary cause?

For a possible answer to this question, let us now turn our attention to a new breed of destabilizing and chaos-producing, non-conventional threats that are appearing throughout the world. These new threats, left unchecked because they are confused with police work, may be the direct cause of the high level of instability and disorder evident in many parts of the world. These threats may increase in magnitude if nations fail to recognize them for what they represent: a non-conventional enemy that leverages inherent asymmetries to gain influence that is out of proportion to its political, economic, and military strength. Traditional analysis is likely to fail to recognize these patterns of new and powerful emerging threats. As a result, appropriate responses may be delayed.

---

[4] Please refer to appendix I for breakout.
[5] Please refer to appendix I for breakout

Left unchecked, the destabilizing effects of these threats could spread, potentially causing the collapse of nations and altering the balance of power throughout the globe. This chapter expands on the concept of asymmetry introduced earlier and advances the thesis that a transformation appears to be taking place that has begun to alter the entire calculus of non-conventional warfare.

C. MODERN ERA, NON-CONVENTIONAL THREATS

1. Overview

While emerging, non-conventional threats are difficult to categorize, they share one readily identifiable characteristic: they break down the order and legitimacy of the state by discrediting its ability to protect and defend its citizens. Once this basic responsibility has been maligned, the state loses relevance and its future is short lived. It is through the resulting chaos that new order threats discredit modern society and overwhelm its infrastructure.

New order threats comprise not a few, simple organizations but hundreds to thousands of different organizations that span a continuum from simple to complex. They are continually evolving so that tracking, measurement and analysis will prove difficult. Modern convention, still predominately tied to Cold War analytic technique, describes the Third World variants of these threats as guerrillas, rebels, human rights violators, warlords, kidnappers, smugglers, etc. The variants appearing in the developed world carry other names such as hackers, gangs, criminals, terrorists, or police work. (Bunker, 1997)

The transformation of the new threat into the modern age is mirroring modern society's economic and technological evolution. Like today's business entrepreneurs, the threats quickly adapt to the market place and find niches where they can succeed. They

use the free, open marketplace to maneuver and democratic institutions as shields. Most significantly, these threats are learning to operate effectively across a new battlespace: the political, economic and mass media battlefield. Not unlike the battlefields from which these threats sprang, the new battlefield is as chaotic and disorderly as the jungles of Nicaragua and the mountain terrain of Afghanistan.

Bypassing military and other security organizations, the new threat lives within the social, economic, and political arena of the enemy's homeland, exploiting its weaknesses and using them to strategic advantage. Not unlike modern corporations, they too must turn a profit. Uniquely positioned to exploit the new battlefield, profit making can be instituted in multiple ways, ranging from conventional terrorist strikes and guerrilla attacks to new era warfare. That warfare is expanding into areas such as reducing the legitimacy of a government, influencing world opinion, or proliferating weapons of mass destruction, narcotics, pornography, prostitution and the like.

Perhaps an effective indicator of the existence of these new threats is the movement of chaos from the Cold War battlefields of Third World nations to the streets of modern society. Many nations in the former Soviet Union are facing this as new order threats proliferate in the political, social, and economic environment:

> Police in Russia estimate that about 3000 organized crime groups, allied into about 150 confederations, now exist and that half of the country's banks and real estate are Mafia owned....These groups control not only traditional criminal activities such as drug trafficking, prostitution, extortion, loan sharking, black marketing, etc..... but also other spheres of influence. For instance, estimates show that 40,000 state run and private companies are controlled by the crime syndicates in Russia. (Bunker, 1997)

This new warfare is still in an experimental form. It is evolving and growing, matching society's technological and economic revolutions. As the world continues to

grow smaller through globalization of markets, economic reform, and advances in technology, the United States and her allies become increasingly more vulnerable to these threat actors. More at risk than the modern state will be the developing world, but as nations battle for resources in the hyper-competitive world economy, confrontation of some sort is inevitable.

What is the anticipated form of such confrontation with these new threats? Direct conventional intervention with the United States appears less likely, given the present and expected future superiority of U.S. forces. More likely is the potential for an aggressor state to contract sub or transnational actors to wage *New Order* warfare. Such warfare would not only be difficult to detect, but, once discovered, its source would be hard to identify. Even if a source could be found, new questions over reciprocity would arise. New rules of engagement would need to be developed as the "enemy" would not fit traditional definitions and modes of operation. Also more likely is the potential for U.S forces to operate in assisting other nations overwhelmed by this new warfare. Whether it is humanitarian assistance or limited conventional intervention, the United States Marine Corps soon will confront these emerging non-conventional threats.

2.   **Origins and Early Evolution**

The Cold War is considered to be the birthplace of the emerging, non-conventional threat. During the Cold War, the two Superpowers pursued policies of détente mixed with limited expansionism. Intent on expanding their influence while at the same time avoiding nuclear obliteration, the United States and Soviet Union sponsored regional actors to advance their cause. Unable to fight each other directly, the

Third World[6] provided the battlespace for the two Superpowers to confront each other indirectly through third party actors.

This Cold War period of intervention fueled many innovations in new order warmaking. While the U.S. and Soviet Union were building huge conventional militaries to confront each other on the plains of Europe, different forms of warfare were proliferating in the frontier regions of Superpower domination. The Third World proved to be fertile ground for American- and Soviet- sponsored groups to resurrect old guerrilla tactics and to innovate new ones.

The Superpowers and their allies fuelled new threats' innovation through two primary means. First, the large contributions of weaponry, money, and training provided resources critical to warfighting and experimentation. Supplied with modern weapons and tactics, new order threats learned new ways to fight. Second, the frequent deployment of modern Superpower militaries to many remote battlefields provided new threats with insights into modern conventional warfare. Witnessing first hand the devastating effects of modern weapon systems, they were overwhelmed by the sophisticated electronics that enabled precision intelligence and complex command and control.

At first Third World threats posed no real contest for Superpower militaries. Conventional fighting is the bread and butter of modern militaries, and billions are spent on procuring the most effective weapon systems and doctrine to achieve success. However, these threats soon learned to avoid fighting on the terms of their modern adversaries. Refining a new experimental form of warfare, they learned key weaknesses and focused their efforts on exploiting them. Turning conventional weakness into a

---

[6] In fact, the term "Third World" was initially used to define those underdeveloped or developing countries not allied with the Communist or non-Communist blocs.

94

strategic advantage, the new threats shifted their objective from the defeat of the modern military to the defeat of its political will. These emerging non-conventional adversaries learned that strategic success came easiest when it had successfully defeated the enemy's will to fight. Functioning across a new operational spectrum, the focus shifted from achieving tactical success on a battlefield to achieving success across the political, economic, and mass media spectrum of war.

3.   Typology of Modern Era, Non-Conventional Threats

The different manifestations of modern era, non-conventional threats seem to reflect the political, social, and economic environment from which they evolve and operate. For example, threats that arise and operate within the inner city look different than those like Mafias and Cartels that operate in sophisticated, modern society. Furthermore, terrorists, whose environment often is steeped in religion and transnational activities, organize and operate differently than either the street gang or Mafias. Hence, there appears to be a high degree of correlation between environment and threat type.

Accordingly, the nature of emerging, non-conventional threats can be characterized by three types that categorize threats based on their operating environment. For purposes of this thesis, the following typology system is used to facilitate discussion. First, three distinct typologies will be used, low, middle and high. Each type is distinguishable by operating environment, organizational design, potential for danger or degree of strength and power and degree of challenge to the social, political and economic institutions of the nation state (see Table 5.4).

Type	Operating Environment	Organizational Design	Degree of Strength or Power	Threat to Nation State
Low-Order	Local	Simple	Low	Low
Mid-Order	Regional	Bureaucratic	Moderate	Moderate
High-Order	International	Decentralized	High	High

Table 5.4. Non-Conventional Threat Types.

The first type of threat is termed "low-order" and operates within very narrow geographic boundaries like neighborhoods. This threat typically involves local actors whose sphere of influence is limited to the lowest level of organized society's political, social, and economic environment. The second type of threat is termed "mid-order" and operates within nation-state boundaries. While the influence of this threat is typically only regional, some mid-order threats have extensive organizations that stretch across nation-states. The third and final type of threat is "high-order" and typically operates across international boundaries. The actions of this threat type are meant to affect the entire global community. Let us examine each of these types in turn to learn different ways new order threats may organize and operate in the twenty-first century environment. This analysis serves to highlight the difficulties Marine ground intelligence will have understanding these increasingly more powerful threats.

a. The Low-Order Threat

Low-order threats operate within narrow geographic boundaries, such as neighborhoods or cities. Manifestations of low order threats include the street gang, thugs, thieves, and many hate groups (see Figure 5.1).

Nature of Threat	Examples of Threat Types	Design of Organization

Low Order Threat	Street Gangs Thugs Thieves Hate groups Religious cults Hackers	Simple
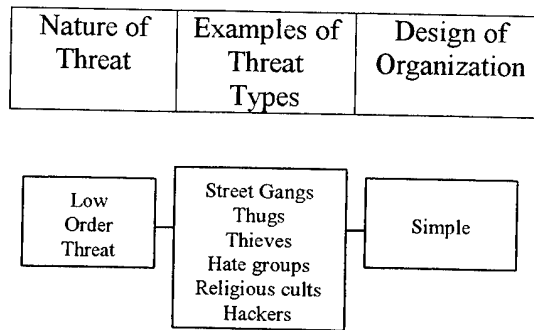
Figure 5.1. Low-Order Threat Types.

The organization of these threats often is a simple, loose structure (see Figure 5.2) composed of ten to fifteen followers and a leader that is haphazardly selected and typically the group's most charismatic member. Command and control in such groups is rudimentary, usually involving little planning and unsophisticated tactics.

Gang Leader		Low-Order Threat -Simple Structure -Loose organization -Haphazard direction -Whimsical operations -Charismatic leader -Operate for thrill, companionship, money
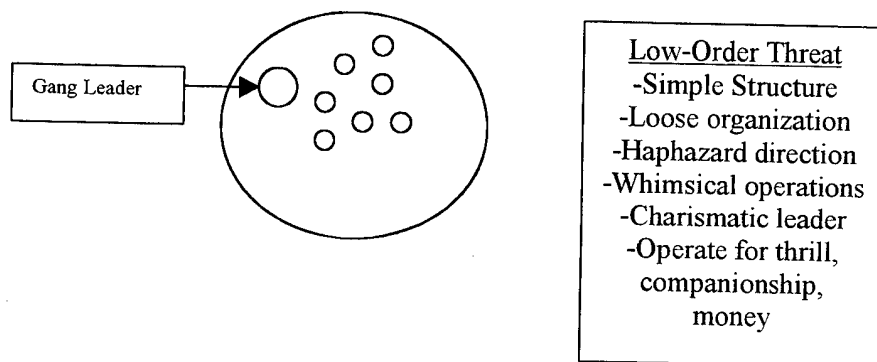
Figure 5.2. Simple Structure of the Low-Order Threat.

Loyalty among group members is varied. However, in most cases it is not strong, and these thugs and gang members are quick to leave a potentially dangerous scene to save themselves. The low degree of allegiance precludes the group from hitting anything but soft targets: low order threats typically attack unarmed, weak civilians and avoid confrontation with law enforcement at all costs. Members are adventure seekers who attack and vandalize for profit and thrill. Civil authority is generally incapable of effectively controlling low order threats, often due to insufficient resources,

97

incompetence, or complicity. In the inner city of developed nations, it may be because of laws preventing effective police work.

b.   The Mid-Order Threat

Mid-order threats are nation-state centered (see Figure 5.3). Examples include private security forces, Mafias, Cartels, and sub-state rogue governments. They typically organize as bureaucracies. Mid-order threats establish large bureaucratic organizations to stabilize and exploit the nation-state environment (see Figure 5.4). These organizations build efficient drug smuggling, prostitution, and gambling operations; they adhere to a strict hierarchy that reinforces the organizations power structure.

Threat Nature	Example of Threat Types	Design of Organization

| Mid-Order Threat | Security Forces Mafias Cartels Rogue Govts | Bureaucratic |
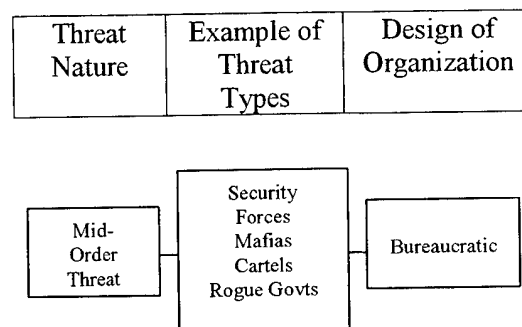
Figure 5.3. Mid-Order Threat Type.

By developing structures be on task specialization, these threats ensure that the required experts run each of the many different operations. These threats generally organize around a task such as drug production, distribution, or other illegal activities. The key motivation for the organization is profit and power. Competition between peer organizations and law enforcement pushes these threat types into clandestine operations.
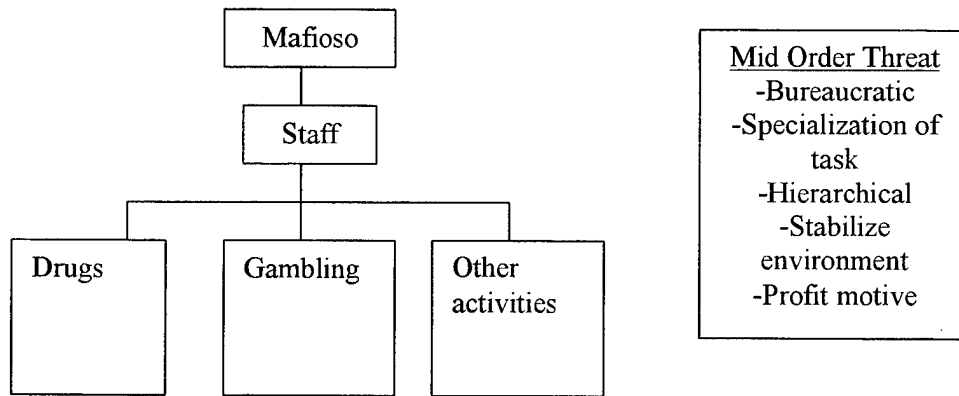
Figure 5.4. Bureaucratic Structure of the Mid-Order Threat.

In an effort to control their environment and stabilize the task of running

the organization, mid-order threats may form alliances with other peer groups; often

times they form partnerships with law enforcement and government. Using specialists

with advanced technologies, the command and control of mid-order threats is capable of

planning and executing relatively advanced operations. In many nations the private

armies of these threats are more powerful than local or national forces; there they operate

with impunity. Many nations in Africa and regions of the Former Soviet Union are

struggling with large Mafias whose power threatens the state both physically and

economically.

c.   The High-Order Threat

High-order threats typically are transnational in nature, and their actions

have worldwide repercussions (see Figure 5.5). Examples of high-order threats include

terrorist organizations, proliferators of advanced technology and weapons of mass

destruction, and trans-state mercenaries.

Threat Nature	Example of Threat Type	Design of Organization

High Order Threat	Terrorists WMD Proliferators Mercinaries	Decentralized
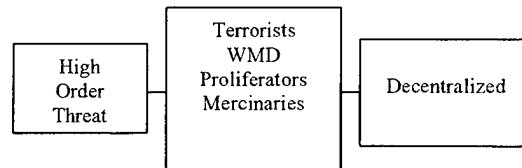
Figure 5.5. The High-Order Threat Type.

The activities of transnational, high order threats demand decentralized

operations and highly trained specialists. Operating far from their safe havens, these

threats are required to survive and operate in the enemy's homeland. To be successful,

these experts must know the goals of their organization and possess the requisite

initiative to act quickly when opportunities arise. These threats are often autonomous

nodes in a highly complex, compartmentalized organization (see Figure 5.6). They are

forced into these organizational types in order to prevent compromise. Because of

security concerns and the difficulties of operating in the world environment, high-order

threat organizations resemble dispersed nodes connected to a central authority. The

central authority determines target selection and resource allocation.

High Order Threat
-Decentralized
-Religious or profit motivated
-Highly trained
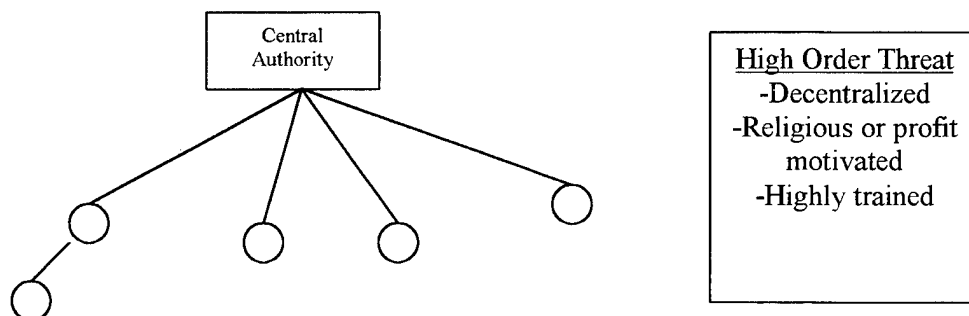
Figure 5.6. The Decentralized Structure of the High-Order Threat.

100

D.   CONVENTIONAL RESPONSE AND THREAT TRANSFORMATION

The previous description of low, mid, and high-order threat types provides an understanding of the initial forms of modern-era non-conventional threats. What might be the impetus and mechanism for the transformation of new threats? This next section advances the theory that these initial forms are catalyzed to transform into more powerful and threatening organizations by the response of society's conventional, dominant, legitimate forces.

At a certain point, a threat may become sufficiently great to challenge the power and legitimacy of established authority, at this point the regime is pressed to wage war against the non-conventional threat. When this "conflict" is set in motion, modern society unleashes powerful law enforcement and military organizations to destroy the threat. Expending large amounts of resources and focusing ultra sophisticated intelligence platforms and collection systems to identify and predict threat locations and operations, society employs its armies of men and material in the battle. Faced with annihilation by the technologically dominant conventional forces, the threat evolves and takes on new forms.

The new threat forms that arise from this conflict with society are transforming the threat landscape of the modern world (see Figure 5.7). Some low order threats are transforming and showing signs of becoming mid-order, networked organizations. Others are evolving into more powerful simple organizations. They form alliances with mid-order threats and harness their unique asymmetries to outmaneuver society. A few mid-order threats are abandoning rigid, centralized structures vulnerable to decapitation and disruption and evolving into network like designs. High-order threat evolution is as of yet

unknown, but it is suspected that it too will take advantage of the new technologies and

organizational designs of the information age. (Arquilla, 1996)

```
┌──────────────┐      ┌──────────────┐      ┌──────────────┐
│   Low Order  │      │   Mid Order  │      │  High Order  │
└──────────────┘      └──────────────┘      └──────────────┘
        │                     │                     │
┌───────┼─────────────────────┼─────────────────────┼──────┐
│       │        Conflict with Society               │      │
└───────┼─────────────────────┼─────────────────────┼──────┘
        ▼                     ▼                     ▼
┌──────────────┐      ┌──────────────┐      ┌──────────────┐
│Need to       │      │Need to       │      │Need to       │
│decentralize  │      │decentralize  │      │decentralize  │
│Movement to   │      │Movement to   │      │Movement to   │
│Network       │      │Network       │      │Network       │
└──────────────┘      └──────────────┘      └──────────────┘

New Org  ┌──────────────┐  ┌──────────────┐  ┌──────────────┐
Forms    │New Order Super│  │  Guerrillas  │  │Net terrorists│
         │    Gangs      │  │New Order Armies│ │Net Proliferators│
         │   Hackers     │  │  Net Mafias  │  │              │
         │  Netwarriors  │  │  Net Cartels │  │              │
         └──────────────┘  └──────────────┘  └──────────────┘
```
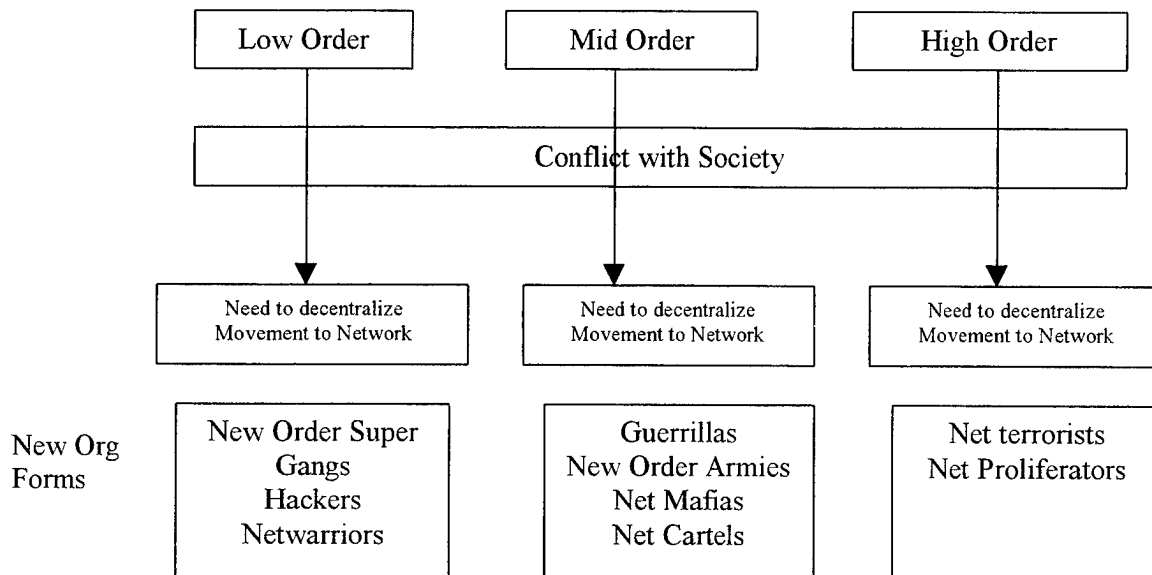
Figure 5.7. Transformation of Low, Mid, and High Order Threats.

The network design presents tremendous challenges to traditional, hierarchical

militaries and law enforcement. Because of its decentralized nature, the network provides

the non-conventional threat with powerful, asymmetric operating advantages. Consisting

of nodes able to operate across large areas with little central guidance, the network is

agile and empowered to make decisions; it can not be easily countered.

Driven by the conflict with society to innovate and transform, low, mid, and high

order threats around the world may be evolving into network designs. The following

analysis of the transformation of street gangs and foreign drug cartels highlights this

evolution into networks and provides valuable clues as to how this process may be

occurring.

102

1. Low-Order Threat Transformation: Street Gangs to Net Gangs

Street gang activity in the United States may illustrate, though particular features will vary with geography and culture, a potential trend in the transformation of low-order threats worldwide. Therefore, the following analysis of U.S. street gang evolution will serve as an example of how low-order threats may transform in response to societal "conflict".

U.S. street gangs are predominately comprised of disorganized, disenchanted youth who see themselves as having little opportunity to achieve status or social identity apart from running in gangs. Generally a phenomenon of disadvantaged inner city sectors, marginalized youth on the whole seek gang life as a means to improve their station in life and to protect their neighborhood. Unsophisticated and possessing little formal education, they typically conduct low technology operations such as drug trafficking and random criminal acts such as shootings and property defacement. As the economic situation has worsened in the inner city, gang populations have swelled in the U.S. In Los Angeles alone there are over 1,300 different street gangs with a total population well over 100,000 members; this figure represents 4.3% of the entire population of the city of Los Angeles (2.3 million). (NDIC, 1996)

As their numbers increase and level of violence grows, gangs have come under intense pressure from law enforcement. Also, peer competition for neighborhood control and lucrative drug markets has intensified. Both these forces have pushed some gangs into new, more powerful operations and net-like organizational forms.

In Los Angeles, Hispanic gang organizations have begun to adapt and change by developing unique collaborative relationships with the Mexican Mafia. A potentially new, highly "sophisticated" enterprise created from the fusion of the street gang and the

drug Mafia may be the outward manifestation of such collaboration to counter increasing competition and police pressure.

Black Chicago gangs have formed an unprecedented alliance that unites hundreds of gang cliques in order to influence and shape a favorable operating environment. In response to increased competition and police pressure, these gangs have begun working together in an attempt to influence society at the political, economic, and mass media levels. They have made progress toward that end by organizing political groups to advance supportive politicians into important posts in government and by gaining legitimate favor from residents by supporting community revitalization programs. By investing in legitimate enterprises, these gangs have transformed themselves from their marginalized status to become inextricably linked to the economy in many inner city neighborhoods.

The following elaboration of these two examples demonstrates that when faced with environmental pressure, gangs adapt and operate differently. While the future evolution of the modern street gang is unknown, it is possible to see how it may transform by studying its present day operations. The next two cases provide important insights into this possible transformation.

a. Los Angeles Hispanic Gangs

In Los Angeles, the gang problem has risen to widespread proportions. Crime and drug trafficking are at all time highs, and homicides have outpaced the national averages. In fact, since 1994, gang-related killings represents, for the first time in history over half of all homicides in the LA region.

A comparison of the national gang-related homicide figure with that of LA demonstrates with striking clarity the degree to which LA surpasses the rest of the

104

country in gang violence. In 1994, there were 1,810 homicides in the United States, of which 779 were gang related. The total number of gang-related homicides in the LA county area in 1994 was 588. Thus, over seventy two percent of the nation's gang-related homicides occurred in Los Angeles. (NDIC, 1997)

The increasing level of violence in Los Angeles has stirred intense public outcry. Consequently, more police have been fielded, and citizen groups have initiated campaigns to rid their communities of gang violence.[7] Other efforts by Federal Agencies such as the Federal Bureau of Investigation (FBI) and the Bureau of Alcohol Tobacco and Firearms (ATF) have focused on forming task forces with local, state, and national agencies to assist in coordination and better share information. (Lopez, 1996) These actions have resulted in record numbers of indictments and prison sentences. However, there is little evidence that suggests gang participation and violence have decreased. In fact, gang-related homicides and crime have increased steadily since 1994, as revealed by a recent LA Sheriff's Department study that indicates that gang violence rose evenly by about 4% each year.[8]

How *did* the LA gangs respond to the heightened attacks from society and the police? There is evidence that early in 1994, in response to increasing pressure from law enforcement and the subsequent loss in drug revenue, the Mexican Mafia began to interact with Hispanic LA street gangs. As the primary supplier of drugs into the LA region, the Mexican Mafia began an effort to loosely organize and influence the operations of the hundreds of disparate LA gangs. The Mafia's first activity in this effort

---

[7] Once such effort as reported by a <u>Los Angeles Times</u> special report on "18th Street Gangs" in November of 1996 (Lopez, 1996) describes how citizens installed video cameras and slung banners across streets advertising anti gang slogans. Apparently such efforts have been successful of ridding gang elements from some communities. The problem is that gangs leave one neighborhood and quickly set up shop elsewhere.

was to order a tactical change in the gang style of operations: instead of drive-by shootings, execute walk-up shootings. By switching tactics so that fewer innocent bystanders would be killed, the Mafia hoped to reduce the number of people affected and thus to relieve the political outcry. The expected subsequent decline in police pressure would permit the lucrative LA drug trade to resume as it had before the conflict with society. While debate exists as to the success of central control over the numerous LA street gangs, the change in the nature of gang-related homicides was significant. Drive-by shootings dropped 36% in 1994 and 34% in 1995. Over this same time period, walk-up shootings increased by 56%.

Other efforts at centralized control by the Mexican Mafia have meet with marginal success. Such control usually means profit sharing within an established hierarchy. Where benefits can be clearly identified, centralized control seems to offer a valid reason for transformation. In other cases it does not, as in the example where several LA street gangs rebelled against the Mafia because it was taking too big a bite from their own enterprises. (Lopez, 1996)

Despite the possible different eventual outcomes, there does exist a clear pattern suggesting that when required, Mafia and street gang can fuse into a single organization. In a confidential bulletin produced by the California State Department of Justice in 1996, a summary statement revealed that "some gang cliques are rapidly evolving from criminal street gangs into more sophisticated groups." As Mafias, Cartels, and other criminal elements come under increasing pressure from law enforcement, they seem to favor the option of employing decentralized, street gangs to do drug trafficking,

---

[8] Quote by Sgt. Wes McBride, project officer for Operation Safe Streets, Los Angeles County Sheriffs Department. Sgt. McBride is considered to be a national expert on gang activities.

racketeering[9], weapon smuggling, and other illegal activities. By outsourcing the actual tasks, Mafias and Cartels limit themselves to command and control functions and avoid exposing themselves to police. This complicates counter narcotics efforts and often frees the Cartel from police pressure while law enforcement contends with gang organizations. While complete, direct control of street gangs from centralized authority may never be possible, financial incentives may be sufficient to encourage marginal obedience. (NDIC, 1996, pp. 20)

Clearly, the effects of Mafia and gang collaboration present serious challenges to law enforcement. The highly decentralized gangs are difficult to detect and they participate in unpredictable activities. Also, as the average age of most gang members is sixteen, effective police work is complicated due to juvenile handling procedures. The introduction of Mafia influence into this already destabilizing threat brings potential professional direction and hugely profitable criminal activity such as drugs and racketeering. If successfully fused, new "sophisticated groups" could emerge whose organizational agility would undoubtedly pose serious problems for modern day law enforcement.

b.   Chicago Gangs

A second example of the evolution of low-order threats in response to conflict with society is found in the street gangs of Chicago, considered to be some of the most organized in America. (NDIC, 1996) More stylized than Crip or Blood Gangs of the West Coast and adhering to traditional gang folklore and symbolism, many of

---

[9]A sweeping federal racketeering indictment filed in 1995 alleges Mexican Mafia leaders collaborated with numerous Hispanic gangs in collecting protection payment from local businesses and dope dealers. The gangs and the Mafia apparently split the money. Such activities have become prevalent as the once steady drug income fluctuates due to effective police work (Lopez, 1996).

Chicago's black gangs are aligned either to the Black Disciples or the Gangster Disciples (two of that city's largest and most powerful street gangs). In the early 1970's, David Barksdale, leader of the Black Disciples, formed an unprecedented alliance between the two gangs. The alliance created a unifying racial umbrella around all allied black gangs, known as "Folk" or "People." Barksdale's merger created the Black Gangster Disciple Nation, which in its heyday was the largest street gang in Chicago. Feuding in the late 1980's created a split, and now the Black Disciples and the Gangster Disciples operate independently and war on each other frequently. (NDIC, 1996)

During their brief union the two gangs created an unprecedented level of cooperation between hundreds of allied gang cliques. In an effort to increase their drug business and other criminal activities in the face of growing police pressure, the mega gang developed a plan to control its environment. Beginning with a campaign to gain widespread favor with residents in the neighborhoods they controlled, the mega gang injected money into community projects[10] and bought and ran legitimate businesses. In this way the gang alliance induced favorable economic growth in many neighborhoods. As this growth was a stark contrast to the squalor that characterized much of the dilapidated inner city, the mega gang's efforts fomented a large degree of popularity amongst inner city residents. Next, the gang initiated a program to influence the political arena and thereby to achieve politically what they could not accomplish themselves in the neighborhoods: a reduction in the degree of police harassment. Supporting local

---

[10] The Better Growth and Development organization is one example of a community program established by the Gangster Disciples. Growth and Development reflecting the sponsors name (Gangster Disciples), this community based organization provides after school day care and sports programs for inner city youth. (Source Sgt. Wes McBride LASD and John Seebeck Chicago Police Department.)

politicians who were well-disposed to their cause, the gangs attempted to elect and influence a number of city aldermen.[11]

Was this effort at gang collaboration an isolated event arising from unique properties of the Chicago gangs? They are not, for Chicago gangs in form are not unlike any other gang or low-order threat: organizationally, they are as decentralized and whimsical as ever. Gangster temperaments preclude cohesive, rigid hierarchies; operating in roving bands of 10-20 members, they operate more out of a desire for excitement than with any real purpose. Each small node or clique is tied to the higher organization by alliance and name only. No centralization of wealth occurs, for profits are rarely shared either downward or upward.

Yet, in Chicago, during this unprecedented period, allied disparate gangs organized to confront an increasingly more effective police presence. Admittedly the success of this effort is highly disputed; however, the fact that many of Chicago's decentralized gang cliques organized to confront increasing police pressure provides insight into the possibilities of these emerging gang organizations. While their nature is fiercely independent, the Chicago gangs' experience may provide evidence that under certain environmental pressures, fragmented gang cliques can unify and contribute to achieving an organizational objective. (NDIC, 1996)

c.   **Alternative Outcomes of Gang Evolution**

Many gang observers are of the opinion that gang movement towards centralized organization is the first sign of the development of a Super Gang (NDIC,

---

[11] The most publicized case was the candidacy of Walter Gator Bradley who ran for city Alderman in 1994. Narrowly defeated, he had known ties to the Gangster Disciples. Bradley was a former convict who sported gang tattoos and openly cavorted with the gang underworld. Source Sgt. Wes McBride LASD and John Seebeck Chicago Police Department.

1996). The delay in the establishment of such an organization may be attributed to the lack of sophistication of present day members. Modern day gangs are too independent and untrusting to pull together and form a cohesive enterprise. Furthermore, charismatic leaders who do manage to rise to the forefront like David Barksdale[12] often experience an early demise due to inter-gang rivalries, intra-gang jealousies, or arrests leading to lengthy incarcerations (NDIC, 1996). In spite of similar maladies, however, the Costra Nostra and other organized crime networks managed to achieve formation. Despite early setbacks, evolution occurred, as it will most likely with street gangs. As with the Hispanic gangs in LA or the black Chicago gangs, such evolution will most likely require severe environmental pressure or competition. Faced with increasing environmental pressure the street gang will either adapt or disappear. Given the continuing economic plight of the inner city, it is unlikely that the social and economic conditions that breed gangs will disappear soon. Consequently, gangs most likely will adapt.

Modern street gang evolution may follow a different course than that of their organized crime cousins who transformed their gangsters into hierarchical, professional crime organizations. Already, Mafias and Cartels are beginning to exploit the agility and nimbleness of street gangs to peddle their drugs, racketeer, and perform other criminal actions. Gang cliques have the advantage of being small, whimsical, and in many neighborhoods so numerous that they far outnumber law enforcement.[13] Difficult to eradicate through traditional police measures,[14] gangs are a unique counter to effective

---

[12] A rival gang member shot David Barksdale to death.
[13] In Los Angeles there are an estimated 100,000 gang members, while there are less than 15,000 law enforcement personnel.
[14] One gang, the Blackstone Rangers was targeted in the early 1990's by the ATF and the Chicago Police Department because of its role as a major narcotics distributor. After numerous arrests and successful prosecutions, gang activity slowed for a short while. However, once police suppression stopped many former members returned and the gang reestablished itself. It now operates under another name. This

law enforcement. It is unlikely that the uneducated and low-skill inner city youth, who are the majority of gang membership, will develop simple street gangs into ultra sophisticated criminal networks. Even with the exchange of knowledge and expertise that may be occurring between organized cartels and street gangs, it is doubtful that street gangs will evolve beyond their current organizational form. Instead street gangs may become the operational arm for more organized interests, becoming, as in the case of Los Angeles, more effective drug distributors, racketeers, and the like. Nevertheless, the Chicago experience reveals that given the right environmental conditions, unprecedented levels of net-like organization is possible among even low order threats.

2. Mid-Order Threat Transformation: Drug Cartels to Net Cartels

Like gangs, drug cartels also have been pushed to evolve into net-like typologies because of the nature of their work, the increase in competition, and effective law enforcement. Consider the monumental tasks facing a modern drug cartel. First the cartel must operate across national borders, deep within hostile nations where police scrutiny and peer competition is often severe. Also, the Cartel must work with a diverse membership that speaks different languages, shares conflicting organizational beliefs, and differs culturally from each other. Furthermore, the Cartel must integrate all of these actors into a cohesive team that can quickly adapt to a hostile environment while at the same time performing the central organizational mission: the production, transportation, and marketing of illicit drugs.

Cartels are able to succeed "partly because... of their emphasis on networks rather than formal organizations" (Williams, 1994, p. 105). Thus Cartels move towards network

---

phenomenon seems to be typical of highly decentralized gang-like organizations. Unless every deviant gang member is imprisoned the culture and folklore of the gang survives.

designs because they provide the organizational framework necessary to perform a complicated task, operate within the chaos of the international arena, and outmaneuver law enforcement.

Organizationally, the modern drug cartel is a decentralized, network-like organization. Often composed of compartmentalized cells that are functionally organized, each generally operates independently of centralized control. Whether producing, transporting, smuggling, or distributing, each function is a node that has "corporate knowledge" and is often free to adjust to its environment. Connected to cutting edge information technologies, these decentralized, functional nodes come to life when their services are required, and then quickly disappear upon completion of a task. However, the drug cartel is a one-dimensional enterprise (Farah, 1997). Focused primarily on drug production, distribution, and money laundering, the cartels have become victim to sophisticated multinational counter drug efforts and peer competition. Furthermore, the Colombian cartels' internal war with the Colombian government has taken its toll on drug operations. Faced with these pressures, Mexican cartels, once minor players in the international drug business, have risen to become the primary drug suppliers to the U.S. (Farah, 1997)

Recently, however, Colombian cartels have begun to alter their organizations to better compete and enhance organizational flexibility and agility to counter anti drug efforts. Searching for more powerful net designs that provide this flexibility and competitive edge, the Cali Cartel has forged a unique collaborative enterprise with Russian organized crime groups. Seeking to gain access to new drug markets, acquire professional expertise and weapons, and enhance organizational learning, the Cali Cartel

and the Russian Mob have joined hands in what is being described as "the most dangerous trend in drug smuggling in the hemisphere" (Farah, 1997).

Unlike the one-dimensional drug cartels, the Russian Mafia is multi-dimensional with hundreds of gangs and thousands of people worldwide operating in many different illegal operations. This breadth of knowledge brings tremendous capability to any Cartel-Mafia joint venture. Comprising highly trained and professional members, the makeup of the Russian mob was characterized by one expert as "people with PhD's, former senior KGB agents with access to sophisticated weapons, people who have already fought real insurgencies and laundered billions of dollars" (Farah, 1997). The Russians also bring to the partnership access to high-technology weapons and equipment. In one known exchange, the Russian Mafia attempted to sell two Russian submarines, several helicopters, and an unspecified quantity of surface-to-air missiles to the Cali Cartel. Since April of 1997, several Russian ships have delivered what are believed to be shipments of AK-47 assault rifles, rocket propelled grenades, and other weapons in exchange for drugs. (Farah, 1997)

The introduction of these types of weapons and technology are changing the entire calculus of counter narcotic warfare. Access to surface-to-air missiles gives the cartel an effective defensive weapon against helicopters, which are used by law enforcement to attack remote cocaine fields, laboratories, and other Cartel outposts. Submarines and armored attack helicopters provides traffickers an almost invincible means of transporting drugs. Use of such weaponry would significantly change the way drugs are transported.

Faced with such newly equipped threats, counter drug work could no longer be a task relegated to law enforcement; trafficker use of submarines and attack helicopters would demand military intervention. As indicated, the Cartels have tremendous tactical flexibility because of their networked natures. Governments like Columbia, Ecuador, Peru, Bolivia, and Mexico are already struggling to grapple with this unique networked menace. The introduction of sophisticated weapons into the equation could topple these fledgling democracies. The recent coup in Cambodia is an example of this.

As another example, drug traffickers bent on transforming Cambodia into a narco-state bankrolled Hun Sen (the co-prime minister who ousted rival Prince Norodom Ranariddh). Sen militarily overthrew Ranariddh in a military takeover in July of 1997. He allegedly secured the loyalty of the military by lavishing gifts and drug money on prominent military leaders. After a brief battle, Sen's forces took power just months after a democratically elected government had been established for the first time in decades. Drug traffickers now operate in Cambodia with near impunity. As a result, Cambodia has grown to become a major transshipment center for Southeast Asian heroin and marijuana. (Thayer, 1997)

The collaboration between the Cali Cartel and the Russian Mafia also adds a new dynamic to organizational awareness and adaptation. Russian criminal organizations "set up cooperative efforts.... they learn from each other and they work together to improve operations" (Farah, 1997). The Russo-Colombian relationship may foster a new degree of organizational professionalism within the Cartel. With the infusion of Russian expertise, the Cartel may learn how to adapt more quickly to its chaotic environment. New methods at countering anti drug efforts could evolve. The already flexible Cali

114

Cartel network design might improve, further complicating counter drug efforts. As already described, the Russian Mafia style of operations is very effective. Comprising former military and KGB personnel, it is difficult to penetrate, and intelligence work is further complicated by the language difference. The fusion of these two organizations could substantially increase the power and effectiveness of both organizations.

The collaboration of the Cali Cartel and Russian Mafia demonstrates the adaptive nature and network centric approach to operations of emerging, mid-order threats. In the case of the Colombian Cali cartel, the collaboration is evidence of the Cartel's tremendous organizational flexibility to adapt to a challenging external threat. For the Russian Mafia, a Russo-Colombian enterprise is yet another signal of the increasing global reach and power of a non-state criminal threat that has yet to be effectively countered by society or a peer challenger.

While the success of these emerging organizational alliances and approaches is uncertain, most law enforcement officials agree that "American and international law enforcement is not organized to fight this threat" (Farah, 1997). Drug enforcement officials are operationally constrained by bureaucratic organizational approaches to operations. Furthermore, foreign governments concerned more with national sovereignty than with tackling powerful transnational drug traffickers often impede collaborative international efforts. Thus, counter drug efforts are rarely able to match the nimbleness of maneuver displayed by the Cartels and Mafias. As these emerging threats gain increasing power due to their inherent asymmetries, legitimate institutions will become more vulnerable. Able to muster vast resources and knowledge from transnational operations and collaborative relationships, the precarious state of nations besieged from

mid-order threats, like Colombia, Peru, Bolivia and Russia are likely to reach critical

mass. They may collapse the nation state and become narco-states where drug warlords

and transnational criminals operate with complete license, as appears to be the case in

Cambodia.

E.   PRINCIPLES FOR RESPONDING TO NETWORK CENTRIC OPERATIONS

Several overriding principles associated with network design and operations are

highlighted by the adaptation and organizational evolution of the LA and Chicago street

gangs and the Cali drug Cartel. The first principle is that the network design is the

quintessential design for threats operating in the twenty-first century (Arquilla, 1996). It

can think faster, respond more quickly, operate more efficiently, and deploy more

effectively than any other organizational design; it is without peer. This is particularly

evident when net-like criminal organizations confront bureaucratic intelligence and law

enforcement.

The second principle is that traditional hierarchical, law enforcement

organizations are ill configured to grapple with networked adversaries. Some

governments have attempted to adapt by abandoning stovepipe bureaucratic methods and

adopting network-like overarching, inter-agency approaches like the task force.

However, while the task force and other similar solutions offer society a way to mirror

the threat's organizational design, their success is often limited due to the many factors

that plague any public agency. Rivalry, lack of interagency cooperation, mistrust, and

misunderstanding are a few of the problems that impede network operations by legitimate

authorities within the U.S. These problems are only compounded when inter-

governmental networks are established.

116

Thirdly, governmental counter drug efforts are still locked in 20th century tactics and paradigms. Massive amounts of resources are spent in capturing suspected "central" leaders. These decapitation operations have minimal effect on networked criminal organizations, yet they remain the focus of many counter narcotic operations (Arquilla, 1996). Such actions are further evidence that modern law enforcement and counter drug efforts are poorly organized and inadequately trained to address networked adversaries.

Finally, it must be recognized that network organizations cannot be defeated; they can only be suppressed. Networks' dispersed, decentralized nature makes them less vulnerable to collapse, and they have amazing empowering effects upon the people that form them. Comprised of a new class of warriors, net-warriors are educated to think and make decisions; they are risk takers and unconventional thinkers. Tied to their network either because of economics, religion, or common cause, net-warriors are loyal to the network regardless of the basis for their affiliation. These features create a network of net-warriors who are powerful, intelligent, and in a sense individual microcosms of the organization.

Attempts by law enforcement or militaries to collapse the network through well-targeted attacks on key nodes may slow the network down, but unless every net-warrior is imprisoned or eliminated a physical impossibility the network will most likely reconstitute itself. Like the gang problem in many inner city neighborhoods, short of imprisoning or eliminating every gang member, the gang seems to always reconstitute itself. Hence, attempting to collapse a networked organization may only temporarily suppress it and achieve short-term objectives; it is not an end all, permanent solution.

F.   SUMMARY

Emerging non-conventional threats present modern society with a perplexing threat picture. To understand the picture, a new calculus for analysis is needed to determine how these emerging organizations fight and wage war. As mentioned earlier, international organizations like SIPRI, IISS and IFRCRC are increasingly less able to explain the level of chaos and disorder that persists despite the fact that the number of conflicts worldwide is decreasing. This confusion is brought about by the tendency of these groups, like many militaries and intelligence organizations, to confound the emerging non-conventional threats with crime or police work. This is understandable, as the threat increasingly looks less like war and more like urban, low intensity conflict. Using Cold War era thresholds like SIPRI's major war thermometer,[15] many policymakers are not seeing the reality of the world environment and remain fixated on watching for twentieth century conventional war to appear.

This is not to say that conventional or even nuclear war has disappeared. Rather it suggests that the emerging non-conventional threats are a phenomenon presenting the modern world with a new threat paradigm that is largely misunderstood. Because of their unique nature, these threats, unlike other forms of warfare, are not expressly tied to a specific form of operations. This fact strains modern threat assessment. Consequently, reams of data are not available to paint a realistic picture of how these threats fight.

However, recent history provides sufficient clues into the operational art of non-conventional threats to provide a reasonable picture of how these threats can be expected to fight; the figure below (Figure 5.8) summarizes the major points of that picture.

---

[15] Recall that SIPRI classifies major-armed conflict as those conflicts producing a 1000 or more casualties.

Threat Evolution	Threat Nature	Examples of Threat Types	Design of Organization	Flashpoint	Adaptation	New Warmaking
T H E C O L D W A R	Low Order Threat	Street Gangs Thugs Thieves Hate groups Religious cults Hackers	Simple	C O N F L I C T W I T H S O C I E T Y	Need to Decentralize Network Org	-Low tech warfare -Operate within mass media spectrum -Operate within political spectrum -Operate within economic spectrum -Non conventional warfare -Exploit and disrupt IT reliance -Operate without constraint
	Middle Order Threat	Security Forces Mafias Cartels Rogue Govts	Bureaucratic		Need to Decentralize Network Org	
	High Order Threat	Terrorists WMD Proliferators	Decentralized		Need to Decentralize Network Org	

Figure 5.8. Emerging Non-Conventional Threat Evolution.

The cases presented in this chapter, drawn from low-order threats like the Chicago and LA gangs, demonstrate that the inherent asymmetries associated with gang operations are difficult to counter using present day law enforcement tactics. Furthermore, the gangs have the potential to form alliances and collaborate with more powerful and highly organized Mafias and Cartels. These alliances may fuel the development of powerful super gangs that evolve to become new mid-order threats like Mafias or Cartels. Or gangs may evolve to become sophisticated, low-level operational nodes for mid or high-level threats.

The final example of the Cali Cartel's collaboration with the Russian Mafia provides evidence of the agility and adaptive nature of a mid-order criminal enterprise faced with severe environmental pressure. Realizing its weakness as a one-dimensional organization, the Cali Cartel's collaboration with the world's most powerful crime group

demonstrates a specific intent to improve its organizational effectiveness and efficiency. Faced with effective suppression from law enforcement, drained by the war with the Colombian government and competition from Mexican Cartels, the Cali group is adapting its organization to better confront its chaotic environment.

The powerful threats presented in this chapter represent a *New Order of Threats* that promise to severely challenge Marine Corps operations in the twenty-first century. New Order Threats assert this challenge because they are difficult to recognize and understand. They put decision-makers in a quandary that results in delay or ineffective response. Left unchecked, New Order Threats harness powerful asymmetric capabilities that allow them to gain influence that is out of proportion to their political, economic, and military strength. Thus, precise intelligence is the key to countering their asymmetric capabilities.

However, given their unique nature, these threats present serious problems for modern intelligence practices. As described in an earlier chapter, Marine intelligence is designed to accommodate simple, predictable adversaries; its present day intelligence methods and systems would be rendered ineffective by new order threat operations.

The next chapter presents a case study of one of the first modern American military contacts with this new class of threat. It highlights how a low-order gang threat evolved in less than a year to become a powerful, networked guerrilla militia that unleashed enough combat power to ambush special forces commandos, repel repeated air and ground attacks, and destroy the UN mission in Somalia.

This Somalia case study offers a perfect illustration of the new, emerging and evolving non-conventional threat theory put forward in this chapter, and it bears out the

weakness of Marine intelligence organization as identified in Chapter III. Unable to

identify much less predict the Somali threat's actions, decision-makers were severely

handicapped and vulnerable. Overwhelming decision-makers with unpredictable actions

and chaos, Somalis exploited American intelligence and operational weaknesses and

achieved asymmetrical advantages that may have given them unparalleled combat

advantages.

VI. AMERICAN MILITARY CONTACT WITH
NON-CONVENTIONAL THREAT: SOMALI CASE STUDY

A. INTRODUCTION

This chapter presents a case study that synthesizes the concepts of the previous

chapters of this thesis. In recounting a sequence of events in Somalia, this case study

illuminates the weaknesses of the current, hierarchical Marine intelligence organization,

makes evident the tremendous power that can be harnessed by an asymmetric force that

embodies the characteristics of decentralized, non-conventional threats, and dramatically

points to the possible new nature of armed conflict facing the Marine Corps in the

coming century.

B. OVERVIEW

One of the first direct American military contacts with an emerging non-

conventional threat in the post Cold War era occurred during the American intervention

in Somalia from December 1992 to March 1995. This contact is significant because it

clearly illustrates how stovepipe, traditional analysis failed to see the threat for what it

was: a *new class of threat*. Left unchecked because of this, this threat defeated the

American military politically and destroyed the UN mission in Somalia. The

predominate lesson derived from this contact is that once confronted with these new

threats, American intelligence is unable to accommodate their peculiar nature.

Consequently, the new threats overwhelm intelligence operations and render them

irrelevant. To operate successfully against these threats, U.S. forces must know and

understand them. As this case study describes, non-conventional threat analysis is not a

trivial matter. Indeed, to describe and track these threats, new intelligence methods and

processes are required. The Somalia case is important because similar interventions where U.S. forces confront these types of threats will likely continue well into the next century, as evidenced by recent deployments to Rwanda, Haiti, Liberia, the Former Yugoslavia, and Albania.

The focus of this case study is the October 3, 1993, Ranger incident in which eighteen U.S. servicemen were killed on the streets of Mogadishu, Somalia. The United States military had superior firepower and mobility, and the soldiers involved were specially trained elite troops. The Somalis were supposedly unorganized, possessed little firepower, and were assessed as marginal threats incapable of launching any sizeable attack. Operating under old, Cold War paradigms, American intelligence failed to understand the Aideed threat for what it was: *a new class of threat*. Years after the furious, almost 24-hour battle, American military intelligence still is struggling to understand an enemy whose nature is so foreign that it is threatens to render intelligence irrelevant or spur massive reform.

Highlighting the stark contrasts between the American military and Aideed's forces, this chapter describes how American intelligence misread the actual situation on the ground because of its near exclusive reliance on Cold War analytic technique and collection procedures.

Beginning with a brief historical summary to frame the context of the events that lead up to that fateful date, the clash between Aideed's forces and the American military is recounted in great detail to illustrate the new class of non-conventional operations and tactics. Because of the nature of this particular threat, the October 3 clash can only be presented from the U.S. perspective. However, sufficient detail can be gleaned from U.S.

observations to provide a fairly complete picture of how Aideed's militia must have been organized for this battle. The chapter will conclude with a brief analysis of Aideed's tactics and their significance in defeating the American raid.

C.   HISTORICAL PERSPECTIVE

Economically, Somalia is one of the world's poorest and least developed countries. It has few natural resources and little economic potential. Politically, it is dominated by clans whose fierce independence and unwillingness to submit to authority has prevented national unity.

Over the last one and a half centuries, Somalia has been ruled by a series of colonial powers including Britain, France, Italy, and other African nations. These colonial powers invested little in Somalia's infrastructure, focusing instead on exploiting the country's resources for their own economic gains. It was not until 1960, after fifteen years as a protectorate of Italy, that Somalia gained its independence.

Somalia's first president, Abdirashiid Ali Shermaarke, led a democratic, clan-dominated government. He was assassinated in 1969, and the Somali army assumed control. The newly created Supreme Revolutionary Council named Army Commander Major General Mohammed Siad Barre president.

Barre quickly consolidated power as the new Somali dictator and established his clan as the ruling faction through force. Supplied by the Soviets, Barre built an army of over 65,000 men, and in 1977, launched a major offensive into Ethiopia to seize ethnic Somali lands. Initially bolstered by success, Barre's army penetrated deep into Ethiopia; however, by 1978 his army was defeated in a series of Ethiopian offensives. Barre's forces returned to Somalia in tatters.

The defeat left Barre's military in ruins and sparked civil unrest throughout Somalia. In an effort to control the fomenting unrest, Barre launched violent military attacks on his opposition "By 1989 torture and murder had become the order of the day in Mogadishu" (Metz, 1993, p. 50). Villages and communities where anti-Barre clans lived were bombed, and the people were massacred.

By 1990 unrest had turned into full-scale revolution. In January 1991, Siad Barre's government collapsed under the pressure of the warring Somali clans. Barre fled Somalia leaving behind a war-ravaged country in which clans fought each other, each attempting to establish itself as the legitimate authority.

The United Somali Congress (USC), the major opposition movement in Mogadishu and central Somalia, announced the establishment of an interim government and proposed that Ali Mahdi Mohammed (Mahdi) be named as the interim president. Former army commander General Mohammed Faraah Aideed, also of the USC, opposed Mahdi and formed his own USC faction. Intense fighting broke out in Mogadishu between the clans supporting these two factions. Eventually, the fighting spread throughout Somalia, with heavily armed clans controlling various parts of the country allied either to Aideed or Mahdi.

The civil war caused widespread death and destruction. Events worsened as a decade-long drought in central and southern Somalia left hundreds of thousands of people starving. Severe malnutrition and other related diseases threatened almost 4.5 million people: over half the population. It was estimated that 300,000 people had died from malnutrition in a three month period, and that at least another 1.5 million were at

immediate risk. Nearly one million refugees had scattered among the neighboring countries. (Metz, 1993)

D.   INTERNATIONAL RELIEF EFFORTS IN SOMALIA

In response to the famine devastating Somalia, humanitarian relief efforts were begun by the United Nations, and by March of 1991 the International Committee of the Red Cross (ICRC) and other non-governmental organizations (NGOs) were fully engaged. A volatile security situation impeded the relief effort and forced the temporary removal of relief personnel from Somalia on several occasions.

1.   UNOSOM

The relief effort became a food distribution crises, and widespread looting of aid supplies, robbery, and armed banditry caused the humanitarian aid activities to come to a near standstill. In response, the United Nations under the direction of Secretary-General Boutrous Boutrous Gali proposed the establishment of a United Nations Operation in Somalia: UNOSOM. UN forces were to be sent immediately to monitor a recent cease fire agreement in Mogadishu and to provide protection and security for the distribution of humanitarian aid. After considerable delays and difficulties with the principal Somali clans, UN forces began arriving in September of 1992.

The security situation continued to worsen. In October and November of 1992, small enclaves in the cities, including the harbors and airports, were controlled by local warlords who refused to comply with their clan leadership. Mogadishu was a divided city controlled by rival militias, each contending for more power and unwilling to submit to the rules of its family clan. UNOSOM troops in Mogadishu were fired upon, and their vehicles and weapons were taken. Relief ships were prevented from docking, threatened,

and even shelled. Airports came under fire; large sums of cash and relief aid were extorted. Several relief workers were kidnapped and held for ransom; others were killed.

During this time, relief supplies piled up in the warehouses and ships offshore, and only a trickle of aid was reaching those in need. According to some estimates, as many as 3,000 persons were dying a day, while the warehouses remained stocked with food (Metz, 1993). Unless the problems relating to the security and protection of relief supplies were resolved, the UN agencies and non-governmental organizations (NGOs) would be unable to provide the necessary aid. (Metz, 1993)

2. U.S. Involvement Begins

On December 3, the UN Security Council adopted Resolution 794 authorizing the use of all necessary means to establish a secure environment for humanitarian relief operations in Somalia. The United States, under the direction of President Bush, intervened "because of the scale of human disaster and the realization that the United States was the only nation perceived by the Somalis and by the regional states as being in a position to maintain neutrality and with the ability to launch the necessary large scale aid operation" (Metz, 1993, p. 50).

A United Task Force (UNITAF) was created whose mission was to establish in Somalia a secure environment for urgent humanitarian assistance. The first elements of UNITAF, spearheaded by the United States, arrived on 9 December 1992. They were joined by elements of the French Foreign Legion, forces from Belgium, Canada, Egypt, Italy, Pakistan, Saudi Arabia, and Turkey. (Metz, 1993)

UNITAF's plan entailed the development of food distribution centers in each of the major areas affected by the famine. By eliminating from the warlords' control what had been a source of power for them, the relief supplies, UNITAF hoped to reduce their violent threat. Once this was accomplished, the military command could then be turned over to the United Nations.

3. UNITAF Operations

When U.S. forces first entered Mogadishu in December 1992, it was a ghost town. Formerly a relatively prosperous African city of a million or so, years of civil war and the recent famine had resulted in a massive exodus of most of the population. Those that remained were mostly starving Bedouins who had come to the capital seeking aid or young men and former army personnel who roamed the streets seeking profit.

At the time, two major clans ruled Mogadishu: Aideed's USC faction and Mahdi's USC faction. The majority of the city was under Aideed's control, while the Italian quarter and areas surrounding the New Port were under Mahdi's control. Each of these men sought to establish a new authority in Somalia with himself as the new central leader. Mahdi's claim was that he had been elected to be the interim leader by the ruling clans following Barre's exile; Aideed's claim was that he was the primary force that defeated Barre and should assume the leadership because of his successful efforts.

Both clan leaders had agreed to set aside their dispute and allow the UN to set up an interim government composed of representatives from all Somali clans. All agreed that the serious issue of providing relief to the thousands dying from the famine was the first and foremost problem that needed to be tackled; "later," it was proposed through a UN brokered plan, a central leader would be appointed. Consequently, both Aideed and

Mahdi submitted to the UN cease-fire and sat back and watched as thousands of American marines and soldiers occupied Mogadishu and the rest of Somalia, delivering tons of food to selected relief sites.

During this period (December 1992- April 1993) the intelligence staffs of all the tactical units involved were focused on three primary threats: landmines, roving technicals,[1] and the Aideed and Mahdi clans. These threats arose from the debris of Somalia's civil war, in which Barre's men had been heavily armed and possessed some of the best Soviet equipment then available. The scattering of war equipment all over the country meant that nearly everyone had a weapon or two; though by far, the majority of the weapons were held between the Aideed and Mahdi factions. Both factions possessed huge caches of weapons comprised of rocket propelled grenades (RPG's), ammunition of all calibers, every class of small arms, a few tanks, and other heavy equipment. To pacify both sides, the UN allowed Aideed and Mahdi to keep their cache sites with the stipulations that they identify the sites' existence to the American task force, allow for periodic inspections, and remove nothing without UN/U.S. permission.

Within a few short weeks after American Marines and other forces had entered Somalia (December 1993), both sides had supposedly come clean. After taking inventory and assessing each of the cache sites, UNITAF came to several conclusions. First, neither clan was deemed to pose much of a threat to UN/U.S. forces for they lacked heavy weapons and equipment in their arsenals. All the tanks, trucks, and other "heavy" weapon systems were in an advanced state of disrepair. Second, all the authorized weapon storage sites were a serious threat for they were filled with tons of small arms

ammunition and weapons. All classes of weapons from Makarov pistols to heavy mortars were stashed in the various Authorized Storage Points.

By January 9, 1993, UNITAF had completed its mission. UNITAF had rapidly and successfully secured all the major population centers and humanitarian assistance was being delivered and distributed without incident. Soon after the food distribution network had been established and the famine crises had been contained, U.S. forces began to disarm the population. This next phase of operations was part of a UN-brokered agreement whereby the country would be disarmed to ensure the continued flow of aid and to set the proper climate for the peaceful transition to Somali autonomy. In further support of that transition, U.S. forces helped in the establishment of local municipal governments, police forces and began rebuilding hospitals, schools and water systems.

Again, during this phase of UNOSOM, both Aideed and Mahdi sat back and allowed the American and UN forces to disarm the populace. Under special provisions of the UN agreement, only specially authorized individuals could own weapons. Aideed and Mahdi were allowed small private forces to act as bodyguards. Also, the NGO relief agencies were allowed to employ Somalis and arm them to provide protection.

U.S. Marine units and other supporting nations actively participated in confiscating unapproved weapons and stopping anyone who brandished a weapon in public. Intelligence efforts focused on identifying unauthorized cache sites. Once a site was discovered, forces were mobilized and the illegal weapons and ammunition were seized. Several thousand weapons of all varieties were confiscated during this period.

---

[1] A technical was a pickup truck like vehicle with a heavy caliber machine gun mounted on it. These weapon systems were used by criminal elements as well as the clans to extort relief agencies and attack enemies.

However, "the more weapons fished out of Mogadishu the more seemed to remain hidden."[2]

By mid January of 1993, UNITAF had deployed approximately 37,000 troops in southern and central Somalia. Because of the number of foreign forces that had joined Operation Restore Hope, the first contingent of U.S. military personnel began to leave on January 19th. The United States' immediate goal was to quickly turn over the operation to a second UN force: United Nations Operation in Somalia II (UNOSOM II). It was not until March 1993 that UNOSOM II took administrative control and military command.

E.   UNOSOM II: PROGRESS TOWARDS DEMOCRACY

1.   Disarmament

UNOSOM II was originally conceived as a peacekeeping operation that called for the building of a secure environment and the rehabilitation of Somalia's political institutions. The United States provided logistical support for this mission as well as 3,000 personnel. In addition to these forces, the United States also provided 1,150 soldiers from the U.S. Army's 10th Mountain Division to supply a "rapid response when specific threats, attacks or other emergencies exceeded the capabilities of other UNOSOM II forces" (Metz, 1993, p. 53). This force was called the Quick Reaction Force (QRF) and was commanded by Major General Thomas M. Montgomery.

One of the crucial tasks that fell to UNOSOM II was the disarmament of all Somali factions and armed groups. This generated hostility from several clan leaders who not only refused to cooperate in the disarmament process but also openly displayed their noncompliance by setting up random roadblocks to frustrate relief distribution and by attacking soft targets. The Somali National Alliance (SNA) and the faction of the

---

[2] Quote from GYSGT Steven Hamby, Intelligence Chief, 7th Marine Regiment, 1st Marine Division.

USC controlled by Aideed were the principal opposition forces to UNOSOM II, and they were resorting to violence to frustrate its efforts. Aideed's opposition to the UN now was arising due to the increasingly less important role he was playing in the formation of a new Somali state. Furthermore, as peace settled across Somalia there existed less of a need for a strongman to dominate the traditionally unruly clan structure. As such, Aideed began to see the UN reconstruction of his country as a direct attack on his clan and personal ambitions at becoming the supreme leader of a new Somalia that "he" had liberated from Barre. The small-scale attacks and open noncompliance during this early period were the beginning signs of a significant rupture of one of the most dangerous and powerful men in Somalia.

2.   Peacekeeping

Concurrent with the activities of disarmament were the UN's efforts to help Somalia establish the political framework necessary for the transition to a stable government. Towards this end, the UN organized a series of Somali Peace conferences held in Addis Ababa, Ethiopia, to assist in the creation of a Somali State based on democratic principles. The Somali conferences held in January, March, and April of 1993 were attended by hundreds of clan leaders representing all of the major Somali clans. In the initial meetings, strong support of clans for one of the two rival Mahdi and Aideed factions was still evident. However, as peace began to return to Somalia, many clans broke with General Aideed and supported the democratic model being developed at the Peace Conferences. The concept of barring any one clan or ruler from dominating state affairs resonated with most of the delegates, who had suffered severely under Barre's regime.

Aideed's popularity was decreasing, and his status was becoming increasingly marginalized by many of his former supporters. As the UN began promising protection and financial assistance to ease Somalia into democracy, Aideed's designs to rule Somalia were falling on less sympathetic ears. At the heart of the Somali Peace conferences was the framing of a new Somali Government. If the Somalis could organize themselves and set a suitable timetable for the establishment of a government, the United Nations would finance the entire effort. At stake were billions of dollars in investments that would flow into a democratic Somalia.

When the Second Peace Conference ended on the 28th of March, Aideed's USC/SNA party had lost significant support from many of the central and southern factions. Aideed left the conference early and never returned. This critically important fact was noticed but hardly understood or attended to by U.S. and UN representatives. Aideed's rejection by his fellow countrymen and loss of support and power was perceived by him to be due expressly to the UNOSOM II initiatives.

With peace restored and the UN military forces ready to protect them, many clans that had previously supported Aideed out of fear now voted against him and elected a federal style democratic government. They had been ruled for twenty-one years under the despotic Barre regime and believed supporting Aideed would only produce another despot.

After the third conference took place in late May, Aideed made several obvious overtures of discontent aimed at U.S. and UN leaders. Then, intent on not being reduced

to a secondary role in any future Somali government, Aideed launched his first serious attack against the UN.

F.   ARMED CONFLICT

The event described below marks the first of a series of armed conflicts between U.S. and UN forces and Aideed's faction that would culminate in a protracted, daylong battle. This initial incident dramatically reversed the direction of the momentum achieved by the UN in helping Somalia find the road to peaceful, self-ruling order. It also demonstrates how poorly intelligence and decision-makers misread the Aideed threat.

Aideed's forces can be initially framed as a low-order, non-conventional threat that harnessed inherent asymmetries of size, decentralization, agility and adaptiveness to counter UN military forces in the streets of Mogadishu. As military pressure increased, however, and Aideed and his leaders became the victims of an intense manhunt, a transformation occurs. The former, disorganized rabble of Aideed's militia is catalyzed by the violent UN response and evolves and adapts to the conventional war dominance displayed by UN military forces and weaponry. This transformation was not detected and left unchecked, Aideed and his militia evolved and developed powerful asymmetries that allowed them to gain influence out of proportion to their political and military strength. Perhaps one of Aideed's most powerful asymmetries ignored or undetected by intelligence and decision-makers was how civilian casualties would gain Aideed popularity and ultimately contribute to his victory over the UN mission.

1.   Aideed Opposes UN - The June 5th Incident

One June 5, 1993, 25 Pakistani soldiers were killed and 54 were wounded in a series of ambushes and armed attacks throughout the Aideed-controlled sectors of

Mogadishu. The bodies of the victims were mutilated and dragged through the streets of Mogadishu.

After an investigation, it was determined that the attacks were part of a calculated and premeditated series of cease-fire violations by Aideed's militia to prevent by intimidation UNOSOM II from carrying out its mandate. In response the UN launched a series of air and ground military actions. Radio Aideed was destroyed as well as several weapon storage sites and clandestine military facilities. Thousands of Somali civilians were killed in Mogadishu during the course of the UN retaliation, strengthening support for Aideed's cause. Somali had been under foreign domination for much of its modern history and the UN forces had suddenly turned into another colonial power. Aideed instead of being a non-factor in Somali policies as its seemed he might become following the peace accords in Ethiopia, became the clear leader of the Somali people facing Western imperialism.

On June 17th 1993, with clear evidence implicating Aideed and his SNA militia in the attack, the UN called on Aideed to surrender peacefully to UNOSOM II and to urge his followers to surrender their arms. Aideed refused to surrender and continued to attack UNOSOM II operations. During this period his power and influence grew as disaffected Somalis, outraged by the UN's military actions, joined Aideed's militia.

After the incident on June 5th 1993, in United Nations Security Council drafted and passed Resolution 837 calling for the apprehension of those responsible. The United States played an important role in the passage of this resolution, which led to the United States taking charge of the manhunt to bring in the clan warlord Mohammed Faraah Aideed.

136

2.   Deployment of Task Force Ranger

Hostilities between UN forces and Somalis increased as the manhunt for Aideed continued. The combined activities of the UN manhunt and the ambitious disarmament mission of UNOSOM II forces posed a direct threat to the clans of Somalia, and they in turn resisted the UNOSOM efforts. On August 8, four US Army soldiers were killed when a command-detonated mine exploded under their vehicle; Aideed's forces were known to be responsible for the incident. After another mine exploded on August 22, injuring six Americans, following this President Clinton announced that U.S. forces would participate in the manhunt for Aideed.

Task Force Ranger (TFR) was given the manhunt assignment. TFR was commanded by Army Major General William F. Garrison and consisted of Delta Force Commands from Ft. Bragg, NC; a Special Forces helicopter detachment from Ft Cambell, KY; and Army Rangers from Ft. Benning, GA. In Somalia, Garrison did not fall under the operational command of MG Montgomery, although they maintained a close working relationship to allow for coordination of TFR operations and the QRF.

3.   Bakara Market Raid - October 3, 1993

In its search for Aideed, TFR relied on information from Somali agents, as other sophisticated collection techniques were useless in tracking the low-technology enemy. Acting on intelligence from such agents, TFR executed several raids into the Bakara Market neighborhood in south Mogadishu. After numerous failed attempts to capture Aideed, General Garrison changed his short term objective and decided instead to capture Aideed's closest military advisers in the hope of pressuring Aideed to come out into the

open. The raid on October 3 was the seventh raid Task Force Ranger conducted in Mogadishu. Like the six previous raids, TFR planned to attack during daylight hours, rely almost exclusively on heliborne insertion and extraction, and gave numerous indications of its impending mission through a flurry of activity at the highly visible airport. (Atkinson, Jan 30, 1994)

The ground tactics of the October 3 raid were also similar to those used in the previous six attempts. Delta Force (part of TFR) was to fly to the objective while members of the Army's 3rd Battalion, 75th Ranger Regiment headed by Lieutenant Colonel (LTC) McKnight would drive to the target. It was planned that, following the capture of Aideed's staff, the prisoners would be transported back to the airport by McKnight's forces due to restricted landing space for the large UH-60 Black Hawks around the target building, while Delta Force would be extracted by air.

The unanticipated chain of events that followed the actual raid will be described in detail and will be shown later in this chapter to have had tremendous implications for UNOSOM II and the future stability of Somalia. The chronology of events below documents the approximately 15 hours of combat operations that occurred on the afternoon and following night of October 3, 1993.

At 1300 a Somali agent reported that Aideed's military advisers were meeting that afternoon near the Olympic Hotel in the Bakara Market area. The agent identified two of the lieutenants by name, Omar Salad Elmi and Mohammed Hassad. TFR planners identified the target building from a Hughes 530-reconnaissance helicopter, with the crew observing the Somali agent as he drove by the building, stopped, looked under his hood, and then drove.

At 1455, MG Montgomery and MG Garrison discussed the impending mission during a hurried phone call. Both commanders agreed that the Bakara Market area was potentially dangerous, with Montgomery telling Garrison ".... That's really Indian country. That's a bad place" (Atkinson, January 31, 1994).

At 1500, Delta's C Squadron and a support element from the Rangers boarded helicopters at their airfield headquarters only to quickly disembark for an intelligence update. As it turned out, the agent that had identified the location of the meeting was frightened during the earlier target reconnaissance and had marked a building that was one block west from the target building. With amended maps, the raid force re-boarded their helicopters and departed the airfield at approximately 1537.

At 1540 the Delta Force assault element of the raid force flew into the objective area on Hiwadag Street aboard four MH-6 Little Bird helicopters. Billowing dust clouds kicked up by the supporting Black Hawks created a "brown out" that blinded pilots and raiders alike. Despite the poor visibility, the Delta assault element quickly jumped from its aircraft and stormed into the building. The Rangers from the support element were not so fortunate; Ranger PFC Blackburn lost his grip on the fast rope and plummeted 40 feet to the street, sustaining serious injuries that required immediate evacuation. The ground convoy, led by the Ranger Battalion Commander Lieutenant Colonel McKnight, arrived at the target and immediately detached three vehicles to medevac an injured Ranger to the airfield.

Between 1540 and 1610 the assault element swept through the building and collected 24 prisoners including two senior Aideed lieutenants. LTC McKnight's Ranger support element was waiting to extract the prisoners by ground convoy.

After loading the prisoners into a five-ton truck, the nine-vehicle convoy departed for the Joint Operations Command Center at the airfield. Relieved of their prisoners, the Delta assault force called for their planed helicopter extraction. Unknown to Task Force Ranger, however, hundreds of gunman from Aideed's militia had converged on the raid site during the preceding 30 minutes and suddenly massed rocket-propelled grenade and small arms fire on the American helicopters.

At 1610, a Somali RPG struck a Black Hawk, call sign Super Six-One, that was hovering overhead and brought it crashing down into an alley off Freedom Road, approximately 300 yards east of the assault objective.

Although this was a serious problem, TFR had developed and rehearsed three contingency plans in anticipation of losing a helicopter:

1. Insert 15 soldiers from a combat Search and Rescue (SAR) Black Hawk to secure and provide medical aid at the crash site.
2. Dispatch a company sized quick reaction force (QFR).
3. Divert the main body of the TFR raid force from the target (objective building) to the crash site.

MG Garrison learned of the crash while hovering over the objective in his command helicopter. He initiated all three response plans almost simultaneously. Task Force Ranger provided the first response with a MH-6 Little Bird helicopter from the raid force that was on scene. The pilot daringly flew down and hovered next to the wreckage, braving a torrent of Somali gunfire. As the pilot flew with one hand and fired a machine pistol out the cockpit window with the other, the co-pilot jumped out and assisted two wounded Delta snipers into the back of the helicopter. This left Super Six-One's two pilots (both killed in the crash and pinned in the wreckage), two injured crew chiefs, and one Delta sniper remaining at the crash site.

The combat SAR Black Hawk soon arrived on scene and delivered 15 soldiers to the crash site via fast rope. With two soldiers still on the ropes, Somali gunman nearly severed the Black Hawk's rotor system from the fuselage with an RPG. The pilot managed to maintain his hover until the last two soldiers were safely on Freedom Road, and then flew back to the airfield to save his aircraft.

MG Garrison diverted the TFR ground convoy away from its route to the airport and back to the crash site. From Garrison's perspective, this probably appeared a simple matter of the convoy traveling two blocks north and three blocks east. From the ground, however, McKnight saw a maze of alleys and streets that were rapidly filling with Somali gunmen. Small arms and RPG fire raked the convoy from all directions, and an exploding RPG round decapitated an American truck driver. With the convoy suddenly in a fight for its own survival, Garrison ordered it to return to the airfield.

Despite the continuing heavy RPG fires, U.S. helicopters remained over the crash site to provide close-in fire support for the soldiers on the ground. Swarms of Somalis surrounding the crash site challenged the hovering gunships, and the sheer number of militia forced gunners to ignore those with rifles and focus on those armed with RPG's.

At 1645 a second Black Hawk, Super Six-Four, was hit in the tail by an RPG while hovering over the crash site. Spinning out of control, the helicopter crashed into a neighborhood approximately one-half mile south of the Olympic Hotel. The four-man crew apparently survived the crash, although what happened afterwards is not clear. The pilot vanished from the crash site and was never seen alive again, while the co-pilot, Chief Warrant Officer Michael Durant, lay trapped and critically injured in the wreckage.

Suddenly faced with having to defend a second crash site, Garrison launched both the QRF Company from the airfield and a small Ranger relief column. Shortly after departing the airfield, both convoys were ambushed by Somali gunmen and were essentially blocked from advancing to the crash sites. The Ranger column turned back almost immediately, while the QRF Company fought successive ambushes for 30 minutes before returning to the airfield at 1914. Neither force had been accompanied by armored vehicles to increase their survivability and firepower.

After learning of the failed ground rescue attempts, the Delta squadron commander allowed one of his Black Hawks, Super Six-Two, to deliver reinforcements to the second crash site. The pilot, Chief Warrant Officer Michael Goffens, dropped two Delta snipers, Master Sergeant Gary Gordon and Sergeant First Class Randall Shugart, in a clearing 100 meters southwest of the second crash site. Upon clearing the landing zone (LZ), however, Goffens noticed the two snipers were having difficulty finding the crash site through the maze of shacks and cactus. Hovering over the site, Goffens directed Gordon and Shugart to the wreckage and remained on the scene until an RPG exploded against the right side of his helicopter. Miraculously, Goffens kept the Black Hawk airborne long enough to make a crash landing at the New Port.

Shugart and Gordon reached the crash site and managed to free Durant from the wreckage. With the air cover gone, however, hundreds of Somali gunmen surrounded the three Americans and closed to within 30 yards of the aircraft. Shugart and Gordon fought valiantly and were hit repeatedly by small arms fire in their vain attempt to defend the crash site. With Shugart and Gordon mortally wounded, the Somalis quickly swarmed the crash site and captured Durant, who was subsequently held in captivity for eleven

142

days before his release. Durant's testimony of Shugart's and Gordon's valor resulted in their posthumous award of the Medal of Honor.

Nightfall came and the fighting continued around the initial crash site. Garrison and Montgomery oversaw planning to launch a third ground rescue attempt from the New Port, using a battalion sized task force consisting of the 10th Mountain Division's 2nd Battalion, 14th Infantry Regiment, a Pakistani tank company, 32 Malaysian Armored Personnel Carriers, and a ten-man detachment from Task Force Ranger. Lieutenant Colonel David assumed command of the task force.

At the crash site several soldiers labored in the darkness to remove the pilot's body from the Super Six-One's wreckage. The Delta squadron commander and the soldiers on site refused to allow the Somalis to claim another American body and would not leave until they could free him. The soldiers found cover in several houses along Freedom Road, some of which still housed approximately 20 Somali women and children. Although these Somalis were not harmed, Somali leaders later claimed that American soldiers held them hostage and used them as shields during the battle. U.S. military commanders later refuted this, citing security concerns for the troops at the crash site and safety concerns of the Somali families as justification for retaining the homes.

At 2324, David's QRF departed the New Port for the first crash site. Leading with the Pakistani tank commander, the QRF encountered a roadblock approximately one kilometer from the port facility. The Pakistani commander refused to lead the column from this point on, resulting in the Malaysian APC's assuming the lead (Casper, 1994). Shortly thereafter the two lead APC's took a wrong turn and were destroyed by RPG fire. The main body continued to move and triggered a second ambush approximately 500

meters farther down the road. The lead tank stopped to return fire, effectively halting the convoy for nearly half an hour. Upon resuming the march, the QRF divided into two elements, Terminator and Tiger. Terminator proceeded towards the first crash site (Super Six One) and Tiger towards the second (Super Six Four).

The Terminator element, carried by Malaysian APC's, encountered sniper fire from the Olympic Hotel and dismounted to engage. They suppressed the Somali fire but sustained three casualties in the process. Gradually working their way towards the crash site over the next hour, they eventually arrived at 0155 and linked up with the Task Force Ranger personnel. They remained at the crash site until dawn, when a HUMVEE succeeded in prying apart the helicopter wreckage to allow them to recover the pilot's body.

The Tiger element arrived at the second crash site at 0145, finding only blood trails leading away from the helicopter wreckage. Somali RPG gunners quickly engaged Tiger's APC's with hundreds of RPG rounds, inflicting several casualties and disabling two APC's. While coordinating air support and direct fires against the Somali forces, the Tiger element used thermite grenades to destroy sensitive equipment left in the helicopter wreckage. The battle continued through the night, with repeated sorties from Specter AC-130 gunships and other helicopter gunships.

By 0700 on 4 October all forces had returned to a hastily prepared aid station in Mogadishu's sports stadium. Initial counts of U.S. casualties numbered 18 dead and 84 wounded; the Malaysians counted one man dead and seven wounded.

4. Outcomes of the Raid

The raid had several immediate results. First, the attack caused the United Nations to call off its manhunt for General Aideed. Simultaneously, this clan leader became a local hero whose prestige and power were heightened for having stood up to the greatest military power on earth. Furthermore, the loss of thousands of Somalis who were killed during the defense and rescue of Task Force Ranger further alienated the United Nations Mission from the Somali people.

Following the raid, UN efforts at patrolling in the streets of Mogadishu were kept to a minimum. UN and U.S. forces kept to their compounds, avoiding any potential conflicts with the Somali population. Task Force Ranger was sent home.

Having suffered an embarrassing number of casualties, President Clinton announced a deadline of 31 March 1994 for the withdrawal of American forces from Somalia. Other nations soon followed suit, and by December it was clear that UNOSOM II was over. All significant nation-building efforts were halted as each of the participating nations prepared to withdraw from Somalia.

Despite his success in ridding the country of interfering international forces, Aideed did not become the uncontested leader of the new Somali State. Anarchy and chaos continued to rule the impoverished nation, and Aideed was unable to dominate the rival clans. He was shot and killed by an assassin late in 1996.

G.   ANALYSIS OF AIDEED'S MILITIA AS A NEW ORDER THREAT

In analyzing the Bakara Market incident, and the events that preceded it, a major question must be asked: How was it possible for Aideed to mount a defense of this magnitude without American intelligence having the least indication?

Understanding the answer to this question will reveal significant clues into emerging, non-conventional threat operations. Most importantly, it will highlight the ineffectiveness of present day tactical intelligence when confronted with these types of threats.

This analysis will begin by first looking at the question of surprise and attempting to provide insight into why American forces stumbled into Aideed's ambush. The analysis will conclude with a brief look at Aideed's suspected defensive plan. By analyzing the complexity of the Mogadishan defense, compelling clues emerge as to the purpose and commitment of Aideed and his clan in expelling the UN from Somalia.

1. Surprise?

Mogadishu is a relatively large city. On 3 October 1993, in less than an hour, Aideed's forces managed to seal off the city with sophisticated and well defended barricades, mobilize thousands of militia, and coordinate the fires of mortars, RPGs, and other weapon systems. In short, Aideed's forces built a highly organized militia and developed a complex defense plan without revealing any of this to American intelligence.

It seems unbelievable that an ambush and defense as complex and large as what erupted that day could have escaped intelligence's attention, for key indications of Aideed's growing power existed since the very day the Marines landed in December of 1992.

Major indications like the vast quantities of weapons that existed in Mogadishu, the military like atmosphere that surrounded Aideed's headquarters, and the high numbers of former Barre military officers and soldiers aligned to Aideed's cause were rampant and hard to misunderstand. Other less obvious but equally important clues existed as well,

such as Aideed's open disaffection with the Peace Process. Additionally, the full scale confrontation that occurred in February 1993 when Aideed's forces suddenly began firing artillery and mortars at Mahdi's forces on the other side of Mogadishu was another powerful indicator that Aideed was not a small, insignificant stakeholder. Most telling however, was the Pakistani incident in June. This and other terrorist-like attacks that occurred from June to September were all strong signals of an increasingly more powerful and discontented Aideed.

Nevertheless, there is little evidence that an accurate assessment of Aideed's strength was made by American military intelligence before the October 3 raid. The conversation between Montgomery and Garrison prior to launching the raid highlights this lack of appreciation for Aideed's power when they refer to the raid site as simply being in "bad guy" territory.

The Bakara Market always has always considered bad guy territory. Almost always congested, it was an excellent environment for gangs of armed Somali men to attack unsuspecting troops who, constrained by the Rules of Engagement, couldn't fight their way out for fear of harming innocent bystanders. Consequently it was often avoided, and little patrolling activity occurred there.

However, what occurred on 3 October proved that this bad guy's territory extended far beyond the confines of the Bakara Market. Indeed, Aideed's militia seized nearly the entire city and effectively sealed it preventing anything short of armored columns to enter. Yet nothing discovered by this author suggests that a full appreciation of Aideed's strength existed prior to 3 October. It is a proposal of this thesis that this absence of adequate intelligence and understanding about the extent of Aideed's power

and influence can account for the element of surprise so obviously experienced by the raiding forces.

2. Characterizing Aideed's Defense

Three salient points emerge from a study of Aideed's ambush of TFR and his ensuing defense of Mogadishu. First, *Aideed's preparations where highly organized and complex.* Second, *Aideed's forces were decentralized and led by experts.* And third, *the ambush was not happenstance: it was a concerted effort by Aideed's faction to attack the U.S. and UN, inflict politically inflammatory casualties, and force a withdrawal.* Aideed knew that striking at America's political will would bring about the collapse of the international effort in his country. His plan was to force this collapse and prepare the way for his restoration as the de facto leader of Somalia.

a. Complex and Highly Organized Plan

Based on the events surrounding the October 3 incident, it is almost certain that Task Force Ranger was ambushed. After six successive and identical raids in less than thirty days, it is not unreasonable to assume that Aideed and his forces had a fairly good idea of how an American attack would be conducted. Furthermore, Mogadishu had been under heavy American presence for nearly a year, and Mogadishan's had grown accustomed to American patrolling tactics and the incessant overhead air traffic generated primarily by low flying helicopters.

Evidence that Aideed had conducted advanced preparations and achieved a high degree of organization among his militia is readily at hand. When Task Force Ranger landed on the Olympic Hotel, Aideed's militia immediately mobilized. It is likely that a brief radio transmission alerting commanders was sent throughout the Mogadishu

cordon. If radio communications were not used, foot or vehicle messengers were probably used instead. In any case, in less than an hour a large and powerful militia began to mobilize, roadblocks were constructed, and mortars and anti aircraft guns were deployed for action.

Other evidence of deliberate planning for the ambush is apparent in the hundreds of swarming militia who immediately converged on the raid site. Firing from neighboring buildings and attacking from adjacent streets, Aideed's militia attacked the main assembly area where the Task Force commandos were exfiltrating via helicopters. During this initial confrontation Army helicopter pilots describe how dozens of Somali's fired volley after volley of RPG rounds at their hovering aircraft (Atkinson, January 31, 1994). When the first helicopter went down within a few short minutes after their attack, the Somali militia seemed to gain confidence and become more daring. Confident because they had been able to down a symbol of American and UN strength, hundreds of militia forces began swarming through the streets firing at any American target. RPG gunners focused on hovering aircraft, while militiamen armed with assault rifles swarmed over the downed helicopter.

While Aideed's militia attacked the Task Force located around the crash and extraction sites, a strategically complex and deliberate defense began to develop around the city to seal the trapped Americans in and prevent any forces from entering. Based on fragmentary accounts, it appears that Aideed divided Mogadishu into distinct sectors. Faithful lieutenants, who more than likely served under Aideed in the former Somali Army, may have commanded them. Once word was given to seal the city, each of the sectors mobilized its forces and established complex barriers to prevent entry into

149

Mogadishu. A sizeable force, armed with many different weapons including RPG's, grenades, small arms, and possibly crew-served machine guns, defended all the barriers. So tight and effective was the defense that nothing short of an armored forced entry could penetrate it. Repeated American attempts to forcibly enter the city were staunchly beaten back by a well-orchestrated militia that wielded a superior amount of firepower and manpower.

During the battle, mortars and one known ZSU 23-2 anti-aircraft weapon system were deployed to support Aideed's militia. One account states that Aideed as central commander maintained the fire control over these weapons. During the fierce night battle where several U.S. commandos sought refuge in houses filled with Somali women and children, mortar fire was requested. Apparently, Aideed denied the fire mission, refusing to fire on a house that may have contained innocent Somali women and children.

In combination with each other, these events describe a highly complex ambush and defensive plan. Organized into sectors, and aware of their distinct missions, Aideed's militia deployed a formidable force that brought Task Force Ranger to its knees and sealed Mogadishu off from outside attack for over 10 hours.

b. Decentralized and Led by Experts

Aideed's militia was greatly enhanced by the number of experienced soldiers that aligned themselves with Aideed's faction. Indeed, Aideed's ambush and defense illustrate all the signs of a highly trained cadre of leaders conducting guerrilla style warfare with untrained, Third World rabble. Themselves trained during the Cold War in various Soviet war colleges, Aideed and his lieutenants were experts on guerrilla,

150

low intensity warfare. Additionally, many of these same lieutenants were combat veterans of Barre's Ethiopian campaigns. These former soldiers brought Aideed's militia military discipline and knowledge that proved instrumental during the 3 October ambush.

The level of expertise leading his forces allowed Aideed to develop a complex defense. Assigning trusted, highly trained lieutenants to the each of the defense sectors, Aideed was able to build a decentralized force that could respond rapidly to any developing threat. Knowing the Americans could jam any radio communications or target radio sites for destruction, this form of organization was crucial to success. Furthermore, the decentralized nature of his force gave local lieutenants tremendous flexibility. This flexibility no doubt contributed to the impenetrable barrier developed around Mogadishu in lightning fast time.

3.   Aideed's Achievement in Non-Conventional Terms

During the battle, Aideed's militia suffered horrendous losses. While no exact body count was ever published, repeated sorties from KC-130 gunships and attack helicopters were launched during the eighteen-hour ordeal. Hundreds of thousands of rounds were fired into Mogadishu's streets. The true body count must have been staggering. Yet, Aideed's battle with American and UN forces was not about conserving forces and fighting another day. Indeed, Aideed fully understood that his rabble of uneducated, poorly trained forces was no match for the technologically superior American Army. Rather, the 3 October ambush was part of a concerted effort, begun months before, to destabilize the UN's position in Somalia and guarantee Aideed's position as Somalia's dictator.

A student of several Soviet war colleges, Aideed was trained in special tactics and knew how to wage war against established power. After all, he had only two years before successfully ejected Barre from power using many of the same tactics he now employed against the American and UN operation.

Marginalized by the Peace Conferences and losing power amongst the clans allied with him, Aideed began a campaign as early as March of 1993 to gain the necessary support to become the next ruler of Somalia. His plans were frustrated, however, by the success of the UN effort. Impressed with the commitment of the UN to rebuild Somalia and establish a new democratic government, many clan leaders turned their attention away from Aideed and supported the UN proposals. By May of 1993 Aideed was finished with the UN. He understood plainly that the political system that was developing in Somalia was not going to accommodate him as supreme leader. Consequently, he began a slow and methodical guerrilla campaign designed to embarrass the UN mission and negatively influence the political will of the participating nations.

This first violent action occurred in June, when 25 Pakistanis were killed in an ambush. Reacting violently, the UN killed hundreds of innocent Somali's in several retaliation raids. By September of 1993, Somalia had been turned upside down. Clans that once wavered in their support again aligned themselves with Aideed's USC faction. In just four months, from May to September, Aideed had risen to national hero status, reversed the popularity of the UN and the Nation Building operation, and had charged the situation in Mogadishu to the boiling point. When the 3 October incident occurred, he had built a sizeable militia and was ready to launch his coup de grace. Acutely aware that American causalities would electrify the American public and create strong political

opposition to continued American operations in Somalia, Aideed framed his attack to produce maximum American casualties, regardless of the cost to his own forces.

The 3 October raid presented the perfect vehicle for Aideed's plan. Twenty four hours later, 18 Americans were dead, Mogadishu was a virtual death trap, and every nation participating in the UN mission was clamoring to get out of Somali. Aideed had won.

H.   SUMMARY

Using the warfare of emerging, non-conventional threats, Aideed and his militia overwhelmed what was designed to be a relatively small scale, precision UN/U.S. operation conducted with the most advanced equipment and most highly trained personnel in the world. The success of Aideed in this particular October 3 incident was dramatically aided by the lack of appropriate intelligence about the nature and magnitude of the threat he posed. This failure to acknowledge a New Order Threat, as described in previous chapters of this thesis, can be attributed to the configuration of an intelligence organization designed for a past era where threats were centralized, predictable and could be monitored and tracked successfully using sophisticated sensors.

Aideed could not be understood because his power did not reside in equipment, technology or organized, centralized forces. Rather Aideed's power centered on his ability to estrange the UN mission and influence the Somali people to take up arms. Therefore, intelligence practices were neutralized and unable to read the Aideed threat for what it was because the traditional signals that alert intelligence were not there. Aideed's forces were low technology and networked. They communicated by messenger and combat power resided in mass human waves of lightly armed people that one minute

would be a crowd at the market and the next a khat crazed stampede of rioting militia. The technology-centric approach to intelligence where sensors and rote intelligence processes dominate, is misaligned with this environment. These emerging New Order Threats do not operate like the threats of the past. They cannot be monitored using only sophisticated sensors and traditional intelligence practices. As demonstrated an intelligence enterprise so configured will fail to recognize and understand these threats. Therefore, New Order Threats will operate unchecked and gain influence that is out of proportion to their military strength.

Accordingly, a new intelligence enterprise must be designed that can recognize and monitor these asymmetric adversaries. The next chapter concludes this work by recommending a new intelligence organization designed to enhance human intellect and create a complimentary interface between the man and machine interface demanded by the emerging threat environment. This network-centric intelligence enterprise shifts the organization from rote information processing to intellect centric, knowledge creation. It does this by pushing responsibility outward, flattening and removing hierarchy, decentralizing and creating a virtual organization that harnesses the expertise of a wide field of experts inside and outside of government. The reader is reminded, nonetheless, that the New Order Threat environment represents such complexity that it will seriously challenge even the network intelligence enterprise configured expressly to meet its challenge.

VII. DESIGNING AN AGILE MARINE GROUND INTELLIGENCE ENTERPRISE FOR THE TWENTY-FIRST CENTURY

A.   OVERVIEW

Marine intelligence is a product of the industrial age. It is configured for the predictable conventional adversaries of WWII and the Cold War. It relies on centralized control, vertical hierarchy and rigid, formulaic processes.

In Chapter IV, Chinese asymmetric responses to American conventional dominance were highlighted. As described previously, both the missile and the reorganization of Chinese ground units represent modern-day manifestations of defense realignment spurred by American war dominance. This push to develop asymmetries presents American forces with serious dilemmas. As they are perfected and proliferate, they render obsolete many of the advantages of American conventional forces. For example, unable to track Chinese forces because they are hard to identify, early warning capabilities are frustrated. Also, missile locations and strengths cannot be identified because they are hidden from traditional monitoring systems, preventing early warning and response. Even tactics cannot be predicted because fighting style is decentralized and unpredictable, creating havoc for intelligence, which must forecast enemy actions. Each of these transformations poses serious challenges to an intelligence organization designed to operate against predictable, regimented forces.

In Chapters V and VI, the inherent asymmetries associated with emerging non-conventional threats were described to underscore their highly adaptive nature and powerful operational capabilities. As mentioned, associated with their unique asymmetries, non-conventional threats are able to organize into network designs that

provide them with significant advantages over traditional law enforcement and modern militaries. Quick to adapt, difficult to detect and nearly impossible to destroy, this threat is spreading and growing more powerful. Not unlike asymmetric militaries, these emerging threats also render irrelevant many of the advantages of American power and technological dominance. Often confused with crime or simple police work, inadequate measures are taken to combat them. Left alone they evolve and form complex, collaborative enterprises with peers that strengthen their operations and make them increasingly more powerful. Because of their unique nature, traditional intelligence practices are unsuitable for tracking and analyzing their actions. As a result, they often go undetected, and when they strike they confound and overwhelm.

Taken together, both asymmetric military and non-conventional threats present a New *Order of Threats* that challenge an intelligence function designed for a the threat environment of the past. In contrast, New Order Threats are, unconventional, networked, agile, adaptable, evolving, asymmetric, non-linear and configured to operate across the political, economic and mass media spectrum. These attributes enable tremendous battlefield advantage. Because of these unique capabilities they overwhelm a bureaucratic intelligence enterprise configured for a different environment (See Figure 7.1).

New Order Threat Environment and USMC Intelligence Misalignment

ASYMMETRIC MILITARY
- Agile, less centralized
- Small and lean
- Sophisticated
- Hi-technology with low technology
- Counter doctrines
  Hardening, Dispersing,
  Multiplying, Confusing
  Responsive war, Blinding
  Over and underwhelming
- Nonlinear, chaos warfare

USMC INTEL
Bureaucratic
Centralized
Regimented
Control
Divisional

NON-CONVENTIONAL THREATS
- Networked
- Operate in political, social and mass media realm
- Adaptive
- Agile
- Difficult to detect
- Evolving
- Unpredictable
- Nonlinear, chaos warfare

Political, Economic and Mass Media Spectrum

Asymmetric

Evolving

NEW ORDER THREAT CAPABILITIES

Non-conventional warfare

Networked

Agile and Adaptable

Figure 7.1. New Order Threats and the Intelligence Bureaucracy.

B. FRAMEWORK FOR ANALYSIS

As presented in Chapter III, Marine Corps ground intelligence is organized

around four bureaucratic elements (centralization of assets and power, standardization of

task, organizational control, and divisional structure) and is currently misaligned with its

operating environment and task.

A parallel misalignment may be found between the American industrial

bureaucracies of the recent past and the changing competitive environment they faced.

Corporate leaders oversaw huge bureaucracies that, like military intelligence, were

centralized, hierarchical, wedded to systems and machines; inflexible, but assembly line

efficient. In the early 1980's, after having spent years perfecting industrial age processes[1],

---

[1] In the late 1970's auto industry executives, frustrated with ever increasing labor costs, designed a system that incorporated the latest advances in information technology in an effort to reduce the need for skilled labor. They built an advanced production control system with decision processing capabilities. Despite

157

these organizations discovered that their structure and operations no longer synchronized with the demands of their environment. American industry found itself in a new era, the information age, which brought with it a fundamental paradigm shift. Knowledge and intellect emerged as the building block for success, displacing the large bureaucratic enterprise designed to manage huge capital and labor infrastructures. Faced with competitors that could produce comparable quality goods at lower prices, many corporations had to adapt or go out of business.

Continuing the analogy, the military can be said to confront turbulence on the battlefield as private industry faces the uncertainties of the marketplace. In interwar periods, however, a fundamental difference between the two exists in that mistakes in environmental adaptation can spell financial disaster for industry, while no apparent impending adversity compels the redesign of the professional peacetime military establishment.

In industry, the stock market and constant competition triggers needed change or validates previous practices, reminding corporations on a daily basis of their need to be flexible and adapt to an ever changing environment. Unsure of what the competition will do or how the market will respond, companies must decide whether to invest in new strategies that could involve billions of dollars. In the hypercompetitive marketplace, successful companies must be agile and uniquely organized to know and understand their operational environment. In the process of conforming to the information age environment, industry has adopted a new paradigm. With rare exception, the success and

---

these efforts, the industry remained tied to a rigid, hierarchical bureaucracy. As a result, the system proved inadequate to meet more efficient Japanese competitors. Tied to bureaucratic processes and design, the centralized authority was unable to keep pace with the market conditions. One analyst observed that "the

158

productivity of firms facing environmental instability, like high-technology industries, lie more in the firm's intellectual prowess than in physical assets like manufacturing plants, property, and equipment (Quinn, 1992).

For the peacetime military establishment, no gauge exists to deliver such overt signals as the stock market sends business. In fact, it generally takes a war to induce revolutionary change in military design and practices, and it is usually only in wartime that such changes can be tested for their efficiency.

The work of this final chapter is to suggest profound change, a paradigm shift, in the way ground intelligence is organized using proven concepts developed by industry in the competitive market place. Two major themes are developed in this chapter.

First, it is argued that intellect, not rote information processing, is the key to properly configuring ground intelligence for twenty-first century warfare. Accordingly, this chapter describes the relationship between intelligence and intellect; it articulates what intellect is, its nature and unique value adding qualities. The pivotal role intellect plays in understanding the increasing demands New Order Threats place on intelligence will be described, making it apparent that ground intelligence must be configured around a technology that seamlessly interfaces both human intellect and machine processes.

Achievement of this seamless interface requires a new organizational design that optimizes the intellectual potential of the organization. Therefore, the second half of this chapter suggests the network as the new organizational form that best harnesses and leverages intellect and systems to respond and adapt to the challenges of a turbulent and chaotic environment.

American auto industry had perfected the methods of fighting the last war and, this time, the Japanese beat the pants off them!"(Macgregor, 1997, p. 35)

C.   THE ROLE OF INTELLECT IN MARINE INTELLIGENCE

1.   Analysis of Threat Types

First, examine the steps involved in the analysis of the four types of military

threats described in this thesis (See Table 7.1). Two of the threats are traditional (a

twentieth century conventional military attack like the Iraqi attack in the Gulf War and a

non-conventional attack like street gang violence or Mafia hits), and two of them are

New Order (an asymmetric military attack like the hypothetical Chinese PLA attack on

Taiwan and an emerging, non-conventional attack like Aideed's attack in Somalia).

For simplicity, the analytical steps have been reduced into four broad categories,

as defined below.

- ❖ *Detection* is the recognition that the enemy is attacking.
- ❖ *Identification* is the understanding of who the enemy is.
- ❖ *Localization* is the understanding of where the enemy is, his intentions and
  capabilities.
- ❖ *Assessment* is the understanding of the enemy's strategy and critical vulnerabilities
  that subsequently enables them to be countered effectively.

THREAT ANALYSIS STEPS	TRADITIONAL THREATS		NEW ORDER THREATS	
	Conventional Warfare	Traditional Non-Conventional Conflict	Asymmetric Warfare	Emerging, Non-Conventional Conflict
Detection	Not Hard	Not Hard	Very Hard	Very Hard
Identification	Not Hard	Not Hard	Very Hard	Very Hard
Localization	Hard	Hard	Very Hard	Very Hard
Assessment	Very Hard	Very Hard	Very Hard	Very Hard

**Table 7.1. Threat Analysis of Traditional and New Order Threats.
After (Berkowitz, 1997).**

The table illustrates that twentieth century conventional warfare and traditional

non-conventional threats are initially less difficult to analyze and become progressively

more difficult. For these threats, **detection** is not hard; it is a simple task to assess that

explosions and maneuver indicate an attacking enemy. **Identification** is almost as easy:

under the rules of conventional war, combatants are required to have insignia and uniforms. With regard to traditional, non-conventional threats, they also typically have recognizable operating signatures. Since membership is a source of pride, it is prominently displayed by the wearing of gang colors or tattoos, etc.

Localization and **assessment** of these two types of threats is more difficult, however. Modern sensors can peer into the battlespace and identify most conventional threats, but processing this raw data into intelligence that explains intentions, weaknesses, and critical vulnerabilities is not trivial. For traditional, non-conventional threats this effort is equally challenging.

While the difficulties of analyzing traditional threats clearly called for capable intelligence, the analytical challenges New Order Threats present are orders of magnitude greater. First, **detection** and **identification** are complicated by the nature of New Order operations. Asymmetric forces, as described in Chapter IV, are configured to counter American technology and military power. Therefore, they quickly adapt to sophisticated sensor technology and other intelligence methods. Burying, dispersing, blinding, confusing and multiplying are some of the techniques these adversaries may employ to avoid detection and identification. Left unable to detect or identify these threats, intelligence is placed in a quandary; and left blind to threat actions. **Localization** and **assessment** are impossible, as the threats very existence is unknown. Left undetected or misunderstood these threats exercise powerful battlefield advantages that afford them great operational capabilities.

Like asymmetric threats, emerging non-conventional threats also employ asymmetry to avoid **detection** and **identification**. However, these non-conventional

161

threats leverage inherent asymmetries like network structures to confound detection and identification. They are also often confused with crime or police work. This is understandable, as the threat increasingly looks less like war and more like urban, low intensity conflict. Because of their unique nature, these threats, unlike other forms of warfare, are not expressly tied to a specific form of operations. This fact strains modern intelligence practices. Accordingly, they operate undetected, making impossible **localization** and meaningful **assessment**. Like asymmetric military threats, this enables tremendous battlefield advantage.

Consider some of the major differences between traditional threats and New Order Threats (see Table 7.2). Traditional threats like the Soviet Red Army were bureaucratic monoliths that adapted to challenges in a slow and deliberate fashion. Taking decades to build weapons, infrastructure, and tactics, the Red Army was additionally encumbered in deploying its massive forces. The mountains of material and equipment along with the hundreds of thousands of soldiers took months to assemble. Detecting and identifying this giant foe was not difficult. (Berkowitz, 1997)

THREAT CHARACTERISTICS	TRADITIONAL THREATS		NEW ORDER THREATS	
	Conventional Warfare	Traditional Non-Conventional Conflict	Asymmetric Warfare	Emerging, Non-Conventional Conflict
Nature of Threat Organization	Large and Bureaucratic	Varied size, Simple or Bureaucratic	Small Lean, Agile Decentralized	Small and Networked
Rate of Adaptation	Slow	Moderate	Fast	Fast
Time needed to build threat capability	Decades	Months to Years	Years	Months to Days
Time needed to generate an attack	Months	Hours	Days	Immediate

Table 7.2. Threat Characteristics of Traditional and New Order Threats.
After (Berkowitz, 1997).

Traditional, non-conventional threats, like Mafias and cartels, are more complex and less easily characterized than conventional threats. While they too, tend to be bureaucratic in form (though at a simpler level), they adapt more quickly to their environment, enabling them to organize rapidly in crises and attack within a few hours. Traditional, non-conventional threats require little time to become threat organizations. In the case of low-order gangs, they can organize within several days; mid-order threats may take several months. These threats challenge and perplex because they are more agile than hierarchical police and military forces.

New Order Threats, on the other hand, are inherently harder to characterize, understand, and monitor. First, New Order Threats are small, lean and networked. They are uniquely configured to hide their identity and actions to counter American technological dominance. Second, asymmetric threat operations enable rapid, high-speed operations that further complicate threat assessment. Thus, their actions confuse and can go undetected.

Asymmetric military forces are small, lean, and decentralized; they execute operations designed to counter U.S. technology and conventional superiority. Their equipment generally consists of off-the-shelf technologies that require little engineering to make them battlefield ready. Consequently the fielding of asymmetric forces requires less time than traditional conventional forces. Due to their small size and agility, they can attack within a few days. This gives them great battlefield advantage, for it makes monitoring more difficult and causes critical indicators, that would otherwise alert and warn, to go unrecognized.

Emerging non-conventional threats present the most difficulty to present-day intelligence practices. Their small, networked organizations, many comprising just a few technically proficient individuals or single operators, make detection nearly impossible. Because of their hierarchy-free design, adaptation by these threats can be accomplished with great speed. As with asymmetric threats, they acquire most of their equipment off the shelf. Therefore, they can assemble powerful capabilities like biological, chemical, and potentially, nuclear weapons in a short period of time. This enables them great operational capability as they can deploy to conduct an attack almost immediately. Most problematic is the fact that networked threats wage war differently than threats of the past. Their weapons are less overt. These threats fight with weapons like small computer discs that contain powerful computer viruses, or with small undetectable vials of chemical precursor, powerful enough to terrorize large geographic areas. As a result, it is difficult to even detect that attack has occurred as the symptoms produced by their attacks are often confused with inner city problems like the drug problem, or, in the case of biological weapon employment, "normal" diseases or epidemics. (Berkowitz, 1997)

Clearly, an intelligence organization that must detect, identify, localize, and assess New Order Threats will be faced with a difficult task. The question arises, given the reality of these threats, what configuration of Marine intelligence would be aligned to meet their challenge? To respond to this question, it is necessary to explore the relationship between intelligence and intellect.

2.   Intellect and Intelligence

Intelligence work is an intellectual enterprise. Simply put, *intelligence* is knowledge about the enemy that is developed from information, which itself is not intelligence but simply unevaluated data like radio intercepts and sensor inputs. Only after raw data is analyzed and subjected to human interpretation does it become intelligence. Intelligence should therefore not be merely an information processing activity where raw information is reworked and repeated. Rather, intelligence should be developed information that gives a meaningful assessment of a given situation. (MCDP2, 1997)

Intelligence, by its nature, deals in estimates and not in certainty. Because information never speaks conclusively for itself; people must interpret and derive meaning from it. Estimating what might be is the most intelligence can ever do, for it is never possible to know everything about a given situation (Schmitt, 1997).

It is a main theme of this thesis that Marine intelligence, like the rest of the Department of Defense, currently spends too much effort on the sensor part or physical data collection aspects of intelligence and is neglecting the intellectual aspects. Even recent intelligence initiatives propose the development of a new class of intelligence in

165

which the intellectual part is removed (Casper, 1997). Termed sensor to shooter intelligence, it presupposes that every target on the battlefield of the future will be sensed,[2] leaving operators or machines the simple task of pushing a button to destroy the targeted enemy.

However, the battlefield of the future will not be so simplistic. Future adversaries will know American collection capabilities and learn to avoid them. While effective ground intelligence of the future *will* require sophisticated collection platforms, these platforms alone will not provide the intelligence necessary to operate against powerful threats. Rather, it will be the fusion of raw sensor data with organizational intellect that "figures out what an enemy is and what he is doing." Intellect is therefore the keystone to a successful Marine ground intelligence enterprise.

For Marine intelligence operations to cultivate and harness intellect, however, requires systematic reengineering. The organization must focus on intellectual processes and match these processes with an organizational design that best leverages them. This type of reengineering is not new to industry: by the year 2000, 85 percent of all jobs in American and 80 percent of those in Europe will be knowledge based (Quinn,1996). The productivity and success of these firms reside in the their intellectual capabilities.

What do knowledge based firms do to leverage intellect? The following section will first examine what intellect is and how it is managed. This will highlight the need for a unique organizational design that optimally leverages intellect to problem-solve. The implications for Marine ground intelligence will be woven into the analysis to

---

[2] Recent experimentation in November of 1996, called Hunter Warrior, conducted by the Marine Corps Warfighting Lab in 29 Palms spent an estimated 50 million dollars attempting to refine sensor to shooter

demonstrate how intellect can be leveraged to transform present-day intelligence design and practices.

3.   Intellect as a Hierarchy of Processes

Intellect is defined as "knowing or understanding; the capacity for knowledge, for rational or highly developed use of intelligence (Quinn, 1996)" Intellect, therefore is the process of human cognition where disparate data elements are transformed through analysis, evaluation, and integration into knowledge. By their nature, data are easy to collect and disseminate. Intellect, unlike data, is generated differently and cannot be easily disseminated. Data is the least useful for decision making; intellect, deployed optimally, allows for deep insight into areas of inquiry and facilitates projection analysis and successful decision making. (Quinn, 1996)

There are four levels to intellect: 1) cognitive knowledge (know *what*); 2) advanced skills (know *how*); 3) system understanding and developed intuition (know *why*); and 4) self-motivated creativity (care *why*); (Quinn, 1992, 1997). As an organization develops and advances up each of these levels, the value of the firm's intellect increases substantially. Successful firms develop all four levels within their organization, thereby exploiting the intellectual capability of their enterprise to create value or profits. (Quinn, 1996)

Marine ground intelligence functions primarily within the lower two levels of organizational intellect. Top level analysts operate at the advanced skill level; they have the tools and knowledge to probe freely into the battlespace. They then react to sensor outputs and fuse this data with previously developed templates or other analytical tools to   ,

---

tactics. Intelligence was reduced to machine processing of targets identified by sensors. This data was then

167

produce information, which becomes the organization's enemy threat picture. Intelligence work below the top level, restricted from inquiring into the battlespace by a bureaucratic organization, is constrained mostly to the cognitive knowledge realm. With few assets, they must rely on higher level analysts to provide knowledge on the enemy and must therefore operate in a reactive mode, merely responding to what they are fed.

Limiting the intelligence operations to the "know what" and "know how" levels of intellect, and not employing the "know why" and "care why" levels, severely handicaps an enterprise. The full intellectual capital of the organization remains underutilized, resulting in less than optimal analysis and problem solving. As described in Chapter III, the intelligence bureaucracy attempts to overcome this by implementing tight control measures and standardized processes, which by their nature restrict intellect and its creation. Intelligence work in the current Marine intelligence bureaucracy is reduced to the processing of information, not the creation of knowledge. The end product is therefore extremely limited in it usefulness, and the organization suffers accordingly.

Intellect has three defining characteristics. When understood and properly exploited, these characteristics can enhance intellect in the Marine intelligence organization by leveraging its brainpower and operating at the most advanced intellectual levels. These characteristics are the exponentiality of knowledge, the benefits of sharing, and the opportunities for expansion. (Quinn, 1996)

Not unlike learning curves, knowledge and intellect grow exponentially when cultivated and developed properly (Quinn, 1996). The more knowledge is taken into the organization and the more opportunities to develop it, the greater the increase in the total knowledge base of the organization. This in turn increases the ability to identify and

---

fed to weapon platforms which engaged the targets.

solve more complex problems. Therefore driving and capturing organizational intellect is key to successfully harnessing an organizations intellectual reservoir. Several examples illustrate these principles.

Arthur Andersen Worldwide (AAW) and McKinsey & Co. are both leading business consulting firms where organizational knowledge is key to success. The accumulated knowledge of both firms resides mostly in the heads of its people or in case teams. To facilitate the development of organizational intellect, AAW has built an electronic interlink that connects more than 82,000 people in 76 countries. This high-speed connection allows caseworkers to create virtual groups around the needs of customers. Thus as one team discovers innovative solutions to casework, this information is immediately distributed throughout the organization. At the conclusion of each case, the assigned team generates an after action report that highlights innovative developments and successfully applied frameworks. Case teams across the organization keep abreast of what each other has learned from the latest assignment. In both these organizations there is a deliberate effort to decentralize learning to the case teams. There is little guidance from the hierarchy and what matters most is the development of individual intellect through practical experience. This focus on developing and fostering organizational intellect is critical to success. Every opportunity is exploited to expose consultants to new knowledge and experiences. (cf. Quinn, 1992)

This example shows how team workers are given responsibility for outcomes at a higher level of intellect. They are required to analyze their case outcomes, evaluate salient points learned, and create an ongoing bank of solution approaches to apply to new cases by communicating effectively with each other. Organizational and individual

knowledge, therefore, increase exponentially. For both these companies the payoffs are enormous, with intellect and its development as the center piece of these firms, both have risen to become extremely successful enterprises.

Knowledge also grows exponentially when shared (Quinn, 1996). "Communication theory states that a network's potential benefits grow exponentially as the nodes it can successfully interconnect with expand numerically" (Quinn, 1996). The sharing of knowledge is powerful. When one person shares with another, a synergy develops to create more knowledge. Questions are raised, answers are provided or challenged, and ideas change and are amplified. When knowledge is shared with one person, this results in linear growth. However when it is shared among a variety of people across different areas of expertise, exponential growth results. Again, an illustration that exemplifies the point: (cf. Berkowitz, 1997)

Recently a heated battle has been going on between the U.S. government and the computer industry over the export of encryption systems using keys longer than 40 bits (Berkowitz, 1997). Keys are numbers that are organized to resist decryption. The fear of the government is that exporting long key lengths would be so secure that U.S. intelligence and law enforcement would be unable to crack them. Commercial software companies like Netscape have criticized these regulations, stating that if the government can decipher their keys, anyone with knowledge and access to high-speed computers can do so as well. Firms like Microsoft, Netscape, IBM, Novell and Oracle argue that no one will buy their financial software overseas if they are restricted to 40 bit key lengths.

In 1994, RSA Data Security, Inc., the leading developer of cryptographic software to the computer industry, decided to organize an exercise to prove to the government that

170

parties outside the government could crack a 40-bit key. RSA posted a solicitation on Internet bulletin boards along with the key and offered prizes to anyone able to factor them. In a matter of hours, a group of computer aficionados across the U.S. and England formed into a virtual group on line to work on deciphering the key. One participant wrote a program that allocated work to individuals and informed key participants as to the project's status. Before the project was completed, hundreds of people had joined the effort, utilizing whatever computer resources they could find (one participant used a fax machine to do some of his calculations). In ten months the team had the answer; the encrypted message read, "This is why you should use a longer key."

When this story first hit the popular press, attention focused on the vulnerability of industry and private citizens. However, the relevant and most significant point here is the *process* that enabled such an incredible undertaking. First, team members separated by thousands of miles self-organized to tackle a complex task. And second, the team shared information on the subject throughout the experience, thus exponentially increasing group intellect and contributing to successfully deciphering the key. Group knowledge shared effectively leveraged intellect to tackle a complex challenge. This is the style of intelligence production likely to be best suited for the 21st century. (Berkowitz, 1997)

Compare this with present-day ground combat intelligence work. Like a slowly moving assembly line, intelligence is collected, produced and disseminated. Sure the systems have changed, (we now have highly sophisticated listening and imaging equipment) but the industrial era processes have not. Take for example a typical intelligence requirement that most ground combat units need fulfilled prior to properly

executing offensive operations. "Where is the enemy?" This request is submitted and processed by several layers of bureaucracy until it reaches the layer where intelligence collection, processing, and analysis are done. Here, an individual analyst will be assigned to the request, and will be limited to only collection assets in processing it. Little knowledge is shared up and down the hierarchy in an effort to clarify or problem-solve collaboratively. Once fulfilled, the result is sent back down the hierarchy to the requesting entity. Naturally, modern information technologies have greatly increased the speed of this information flow. However the process of producing intelligence in a centralized-detached fashion is inconsistent with the sharing of knowledge and the leveraging of intellect for problem solving. Therefore, the end product is likely to be less than optimal, degrading the decision making options for the battlefield commander.

Finally, there are four fundamental properties of intellect that describe how it expands and adds value to an organization that properly harnesses it. 1) Intellect increases with use; 2) it tends to have underutilized capacity; 3) can be self-organizing; and 4) it is greatly expandable under pressure (Quinn, 1996). First, intellect expands with experience. As organizations deploy their intellectual assets against problems each individual involved is afforded unique opportunities to develop cognitive approaches to problem solving. As experience increases, individuals more readily develop frameworks to approach problems; soon expertise develops. Experts can tell the background from the foreground and can quickly sift through data to get to core issues. As experience increases organizational intellect tends to increase exponentially, and as experts from other knowledge areas are included, their input can create steeper exponentials.

Next, organizational intellect is difficult to harness and often goes underutilized. Transitioning an organization from controlling to leveraging intellect demands organizational reform. Even organizations that have sought new intellect enhancing designs do not utilize their full intellectual potential. The full capabilities of human brainpower are little understood. What is understood however, is that nurtured properly it can be exploited to solve complex problems.

Intellect also can be self-organizing (Quinn, 1996). When given proper opportunities and a nurturing operating framework, individuals confronted with complex tasks will self organize into ad-hoc *networks*. These groups of experts will muster with minimum formal organization, but generating a network synergy that will maximize problem-solving intellect. Finally, when confronted with pressure, intellect expands. Much research has been conducted to determine the performance results of intense training, mentoring, and peer pressure within professional communities like law, business, engineering, and medicine. In general, people who face intense 100-hour work weeks in school, go on to intense internships, and then to demanding work environments are more capable and valuable in the performance of their jobs than those who faced lesser challenges (Quinn, 1996). The best intellectual enterprises create environments where intellect can be stimulated and pressured to expand (Quinn, 1996).

D.   LEVERAGING INTELLECT

A decisive factor in the capacity to leverage intellect is an organization's ability to focus on those activities that create uniquely high value for its customers (Quinn, 1996). For the military intelligence organization, the customers are the consumers of intelligence products, in other words the battlefield commanders (division, regiment, battalion, and

company commander, etc.) What activities are unique to the intelligence organization and contribute most to what is desired by its customers? This section discusses what these activities, called *core competencies* are and then examines them in depth to determine the extent to which they currently are configured and use personnel in a manner that exploits intellect.

1.   Value Chain Analysis

For maximum leverage of intellect, an organization should concentrate its resources and executive time around its core competencies so that it can perform them at best-in-the-world levels (Quinn, 1996). If an organization's overall function is thought of as a collection of activities that combine to produce a product, each separate activity should be a significant source of value in the overall process. Value chain analysis is a tool that disaggregates core competencies into intellect-based and non-intellect-based activities. This is important as it aids in identifying those key intellect-based resources that contribute most to the organization. These activities can then be scrutinized to determine how they are performed and whether they add value to the organization.

For intelligence this means uncovering the intellectual-based resources like expertise, knowledge basis, or systems that best provide combat decision-makers with the intelligence they need to fight and win (Quinn, 1996). These resources (instead of actual products or sensor platforms) are what create the level of intelligence demanded by warfighters. By developing these activities and limiting non-value adding pursuits, Marine intelligence can best leverage its intellectual resources into what it is supposed to do: provide combat intelligence.

Figure 7.2 illustrates a broad value chain analysis of Marine ground intelligence. The Primary Activities portion of this diagram represents those activities that contribute directly to the organization's core competency, battlefield intelligence. They are concerned with the physical creation of intelligence, its dissemination and maintenance. The support activities do not contribute directly to battlefield intelligence, but they assist the primary activities and each other. Since the support activities are primarily important to the extent that they support and develop core competencies, they are omitted from the ensuing discussion.
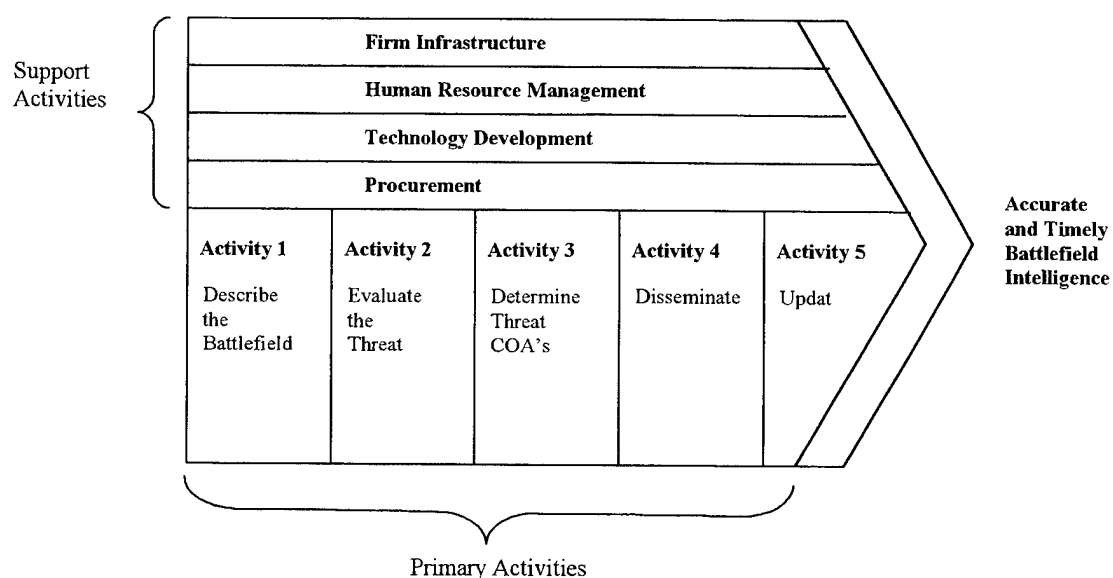
Figure 7.2. Intelligence Value Chain, Primary and Support Activities.

The primary activities of intelligence focus around the battlefield, the enemy, the dissemination of intelligence and its upkeep. Each primary activity is continuous and iterative. Intelligence work fuses all of them together to form an accurate battlefield assessment of the enemy and his intentions. In activity (1), the **battlefield is scrutinized**. This activity involves identification of how the battlefield environment will influence friendly and enemy operations. Examples of possible environmental conditions include

175

such factors as the effects of weather and terrain on maneuver, and the impact of politics, civilian press, and demographics on enemy and friendly forces.

In activity (2), the **enemy is evaluated**. Here intelligence work seeks to determine how the threat organizes for combat and fights. When fighting a known threat, historical data is used to build an assessment of the enemy. However, when operating against unknown threats, this evaluation must developed as contact is made. Each contact must be carefully scrutinized and the data *is analyzed for patterns and distinguishing characteristic. After a* thorough analysis, hypothesis can be drawn which are used to develop conclusions on how the enemy fights.

In activity (3) the **enemy courses of action (COA's) are developed**. This is where intelligence work fuses the results of the previous steps together into a meaningful conclusion. In other words, given the identified effects of the environment and the evaluation of how the threats fights, intelligence analysts synthesize this into meaningful knowledge about what the enemy's most likely activities are expected to be. Once these conclusions are drawn, this knowledge (intelligence) can be used to drive warfighting.

Accordingly, activity (4) is **dissemination**. Dissemination of knowledge is not trivial. It is not simply copying a brief to a distribution list. It must be specially packaged to convey meaning quickly and accurately.

Finally, in activity (5) the process is **updated**. Because combat conditions are rarely static, the previous four activities must be constantly repeated to maintain an updated enemy picture.

Having identified and briefly explained the core competencies, we can now proceed to examine their performance in greater detail to determine whether Marine

intelligence is optimally configured to leverage its intellect. We will first break down the primary activities of intelligence into sub-activities to facilitate further study. The sub-activities involved in **describe the battlefield** are displayed in figure 7.3.

| Collect data on Terrain | Terrain Analysis | Collect data on weather | Weather Analysis | Collect data on battlefield | Battlefield Analysis | Battlefield Effects |

| Human intellect process |
| Machine process |
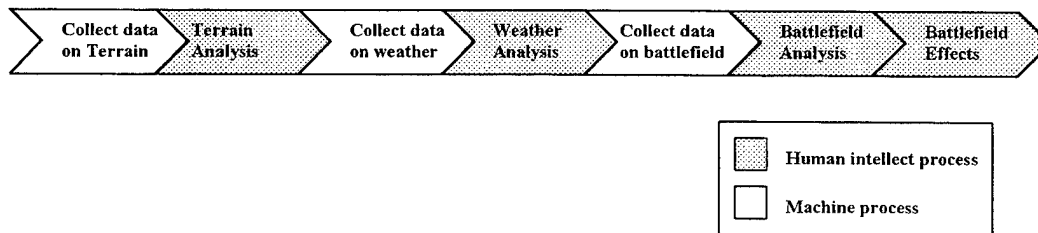
Figure 7.3. Value Chain, Describe the Battlefield.

Note that of the seven broad sub-activities that contribute to describe the battlefield, three activities are shown in white and represent those conducted primarily by sensors and machines. The four activities shown in gray require human intellect for analysis. There is an alternating pattern between sensor/machine activities and human intellect activities, where the systems and sensors first collect data (e.g., on the terrain of the battlefield or on the weather) and then humans interpret and analyze that data to create knowledge. This diagram underscores the complementary interface between machine and human; they are distinct processes but they are interdependent.

Now observe the value chain analysis for the next two core competencies of Marine intelligence - **evaluate the threat** and **determine threat courses of action** (See Figures 7.4 and 7.5).

| Collect data on Enemy | Create Threat Model | Create Templates | Analyze Tactics | Identify HVT's | Identify Capabilities |

| Human intellect process |
| Machine process |
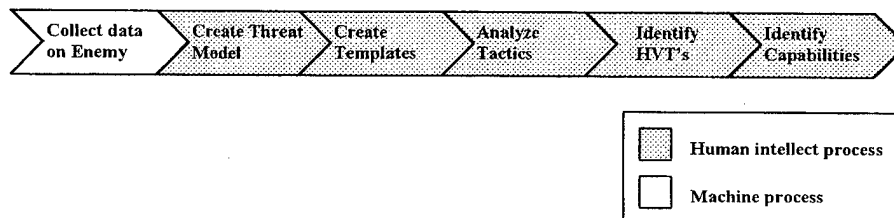
Figure 7.4. Value Chain, Evaluate the Threat.

| Collect data on Enemy | Identify Enemy Objectives | Identify COA's | Evaluate COA's | Prioritize COA's | Develop COA's | Create Collection Plan |

Human intellect process

Machine process
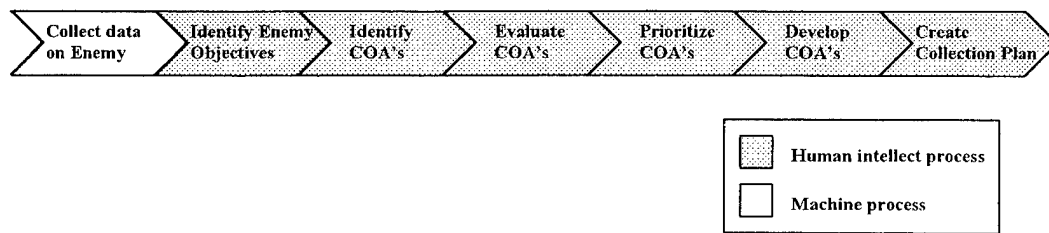
Figure 7.5. Value Chain, Determine Threat COA's.

Both of these primary activities begin with a sub-activity that is a machine function, the collection of data. Once collected, the data is then analyzed in a series of detailed steps that demand human intellect to extract interpretation and meaning. Again, as in **describe the battlefield**, both machine and human interfaces are complementary. In other words, *in concert, they produce a product that neither could on its own.* Without raw data, analysis would be impossible; with only raw data, facts, not intelligence, is the product.

This value analysis reveals two things about intelligence work. First, it is a highly intellectual endeavor that demands a complementary interface between both man and machine. Also apparent is that human intellect, not machines or sensors perform the bulk of the sub-activities. And second, Marine intelligence is ill configured to leverage its intellect to produce the level of intelligence demanded by modern warfare and the emerging threat environment.

The centralized, bureaucratic configuration concentrates the core intelligence activities at the top of the hierarchy, wasting much of the intellect of the organization. Here, only the intellect of a dozen analysts is leveraged by the command level of processing while the remaining organizational intellect sits dormant, dependent on higher

178

for intelligence. In this configuration the three characteristics of intellect described previously in this chapter are not exploited.

Only the few, top-level analysts experience **exponentiality of knowledge** because all collection resources are at the top. The cores activities, all of which are extremely complex and time-consuming activities are limited to a handful of compartmentalized individuals. Also, little **sharing of intellect** takes place during intelligence creation, due to a rigid hierarchy that impedes vertical and lateral communications. Finally, the **opportunities for expansion** are greatly reduced, because only the few analysts at the fusion center are able to ever see the full picture.

In this configuration, the end product of the intelligence bureaucracy is often not intelligence but processed data. Indeed, overwhelmed by the demands from below and the complexity of the task, analysts are hard pressed to spend much time leveraging intellect. To compensate, the bureaucracy reduces this inherently intellectual enterprise into a series of information-processing tasks. Thus for the sake of expediency and efficiency, intellect is subordinated to rote processing of sensor data. Analysts simply do not have time to think much about what they are doing; all they know is that the data is coming in fast and must get processed and disseminated quickly. In effect, machine processes take control of intelligence, and operators simply rework and disseminate its output.

This dysfunctional interface between man and technology reduces a highly intellectual activity, in which intellect is the key component, to a secondary, as time permits, activity. The shuffling and processing of collated sensor data consumes the operator, preventing the level of intellectual analysis required of a complex activity.

Because the bureaucratic design centralizes intellectual processes at the top of the hierarchy, technology drives the pace and composition of intelligence work. This overwhelms human operators' activities when what should be taking place is human operators commanding the technology.

Think back to the value chain analysis of the three primary activities of ground intelligence, and recall the man and machine interface. Each primary activity entails a sequence of sub-activities that demands a seamless interaction between steps conducted by machine and those performed by people. Fused together, man and machine contribute to battlefield knowledge and intelligence. However, when machine drives the human, data is only transferred from one form to another. Raw data is reworked and repeated throughout the organization, with an end result that is not battlefield intelligence.

In today's New Order Threat environment, intellect-based intelligence is more critical than ever before. As presented, however, Marine ground intelligence is not configured to leverage its organizational intellect. Configured as an intelligence bureaucracy, machine processes dominate, and intellectual activities are reduced to information-processing ones. The three fundamental characteristics of intellect, **exponentiality, sharing,** and **expansion** are subordinated to the demands of efficiency. Indeed, the effort to avoid becoming overwhelmed takes precedence over everything, even intellectual activity. But the experience of industry and the emergence of new technologies and business approaches now enable such organizations to capture, develop, and leverage intellectual resources successfully. Such an effort requires reengineering of the organization. The key to such a transformation is designing the organization and

developing information technologies around intellectual flows rather than command and control concepts.

2. Organizing around Intellect

In the past, to enhance production efficiencies, most organizations were designed around product clusters, work processes, geographical needs, or function (Quinn, 1996). Thus, the bureaucratic form arose and became preeminent during the industrial age. Less focused on the needs of the customer or the professionals who worked within the organization, this form of organization optimized the capacity of power holders to direct and control their organizations (Quinn, 1996). Specific command and control procedures, reinforced by rigid hierarchies, were developed to reinforce this *power structure*. For the Marine intelligence bureaucracy, a rigid command and control hierarchy organized around work processes ensured efficient use of limited intelligence assets and resources. As the demands of the warfighter of the time were attritionist and therefore required less detail, this design worked satisfactorily. Examine Figure 7.6 that depicts an attrition era intelligence demand and its accompanying command and control (C2) process. (The bi-directional arrows depicts communication moving up and down the hierarchy.)

Attrition Era Intelligence Demand and C2

Intelligence

An attacking Regiment asks
  Are there enemy in the area?

C2

  Step 1: Request goes to Division.
  Step 2: Request goes to MEF.
  Step 3: Request filled and sent to Division.
  Step 4: Answer provided to Regiment; yes.
  Step 5: Battalion informed of probable enemy.

MEF G-2

Division G-2

Regiment S-2

Battalion S-2
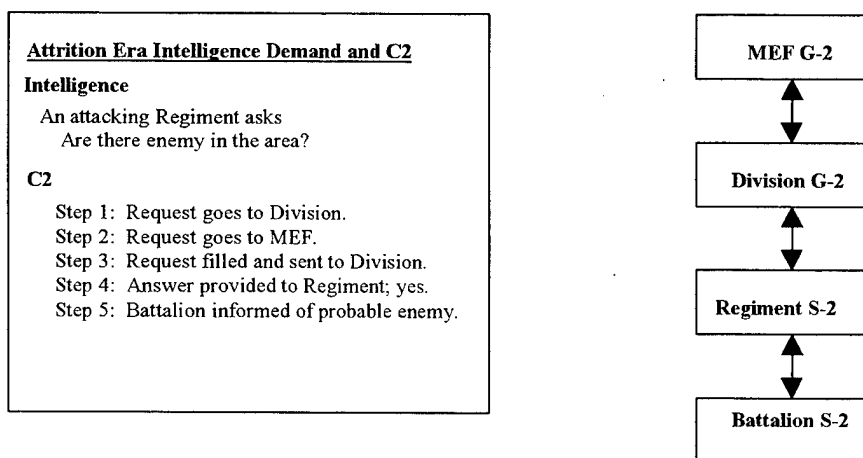
Figure 7.6. Attrition Era C2 - Processing Attritionist Intelligence Demand.

181

The intelligence demand is simple: "Are there enemy to my front?" Remember from previous chapters of this thesis that attrition tactics do not demand precise intelligence; attritionist battles are won through the massing of men and material. Where intelligence aids in directing the attrition army where to fight, it need not inform about how to avoid strengths and exploit weaknesses. Accordingly, the C2 structure can easily accommodate the transfer of this form of intelligence. However, the intelligence demands of war by maneuver and the complexities of New Order Threats require entirely new structures. Examine figure 7.7 which depicts modern day maneuver warfare intelligence demands and the limits placed on them by an attrition era command and control process.

Maneuver Warfare Intelligence Demand and C2

Intelligence

An attacking Battalion asks
  Where is the enemy? How is he deployed?
  What are his most likely COA's?
  What reinforcements does he have?
  What are his artillery and air capabilities?
  Where are they and will they effect me?
  Need updates to this constantly throughout
  the battle.

C2

Step 1: Request goes to Regiment.
Step 2: Request goes to Division.
Step 3: Request goes to MEF and is assigned to an analyst.
Step 4: Some answers provided others data is unavailable.
Step 5: Partial answer to Division.
Step 6: Partial answer to Regiment.
Step 7: Partial answer to Battalion.
Step 8: Update on enemy from MEF to Division
Step 9: Update on enemy to Regiment.
Step 10: Update on enemy to Battalion
Step 11: etc.

MEF G-2
Division G-2
Regiment S-2
Battalion S-2

Figure 7.7. Attrition C2 Processing Maneuver Warfare Intelligence.

Observe the complexity and volume of the intelligence clogs the C2 flow. The contrast between Figure 7.6 and 7.7 highlights an important point: attrition era C2 design

design and practices are overwhelmed by the detailed, precise intelligence that modern
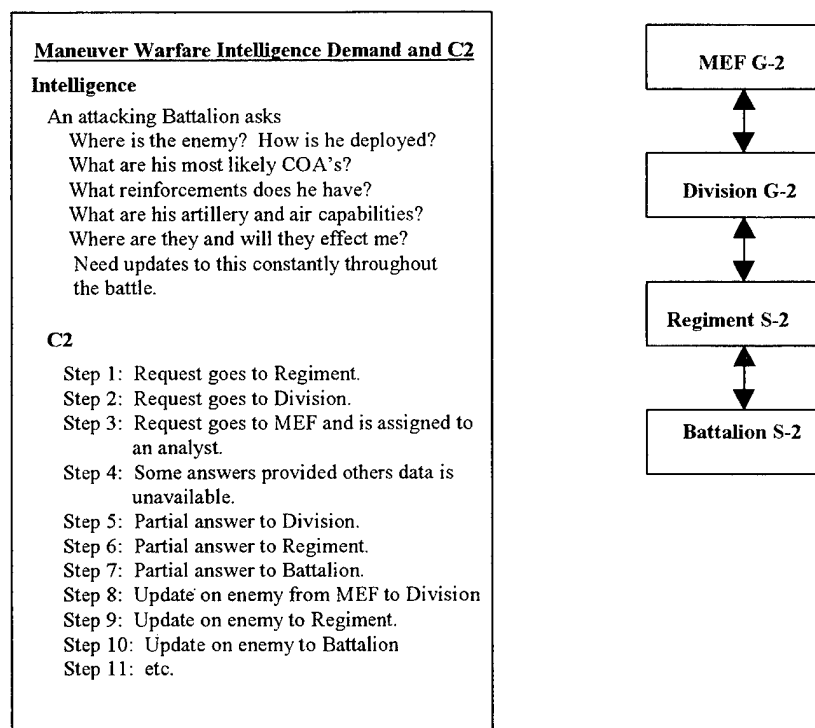
sensors provide and maneuver warfare demands. Designed to support attrition era

operations, not maneuver warfare, the hierarchical C2 practices become overwhelmed by

the massive amounts of information age intelligence. An account of a recent exercise will

provide additional evidence of this mismatch between organizational design and the

intellectual activity it is supposed to support.

During a recent exercise[3] the maneuver warfare intelligence demands of a LAV

Company, combined with the abundance of information age intelligence that was

generated, overwhelmed the C2 system. So abundant was the intelligence generated that,

left unsupervised, the S-2 could easily have clogged the communications TAC 1[4] net with

relevant information throughout the exercise, denying TAC 1's use by other agencies.

Equally likely, the company commander could have remained glued to the radio,

awaiting the near instantaneous intelligence updates that characterize modern collection

sensors. Thus, tied to centralized C2 processes, the company commander and the

battalion tactical net became overwhelmed.

On day 1, prior to contact with the enemy, the intelligence officer passed over the

TAC 1 net an abbreviated report describing four enemy positions to the company's front.

Needless to say, ten minutes later the company made contact with the enemy and

reported several vehicles lost in separate engagements. During the debrief, the company

---

[3] ASCIET 97. Please refer to Chapter III, footnote #7 on page 50 for a complete description of this
exercise.

[4] The primary communications pipe is the Tac 1 (tactical -1 meaning primary or command net) net that
connects battalion with the company. A similar communication pipe connects battalion intelligence with
regiment and so forth up the hierarchy (Called the Intel Net). For this example it is important to know that
there is no unique communications infrastructure to support a detailed intelligence flow from battalion to
the company. In effect, one man, the commander, is forced to fight his company, coordinate fires,
maneuver, report to battalion and finally receive detailed intelligence that demands the plotting of enemy

indicated first that it hadn't received the intelligence, and finally later that it had but didn't

take the time to comprehend it. The company commander stated he was too busy

fighting his company to process, analyze, plot, and disseminate a lengthy battalion

communiqué. ASCIET 97 involved one maneuver company. In combat, a typical

battalion has three companies. The problems encountered during ASCIET 97 easily could

have been compounded by an order of magnitude of three.

The extended capabilities of new technologies and the successful experience of

many corporations in private industry now shed light on design and management

approaches that overcome these antiquated C2 problems and enable organizations to

leverage intellect to respond effectively to the challenging demands of its customers. For

ground intelligence, this means an intelligence organization configured to respond to the

demands of maneuver warfare and capable of operating against New Order Threats. The

term *network organization* has been used to embrace a variety of these new forms that

push responsibility outward, flatten and remove hierarchy, are faster and more responsive

to the demands of the customer, and are agile to adapt to the chaotic and ever changing

environment. The network organization breaks away from traditional command and

control and machine processes as the keys to success and reorients the organization

around intellectual based process (Quinn, 1996). The main function of the network

organization is to develop and deploy (i.e. attract, harness, leverage, and disseminate)

intellect effectively (Quinn, 1996). It is just such an organizational form that will be

explored in the following section.

---

positions on a map while at the same time his vehicle is bouncing around as he maneuvers on the
battlefield. This is very similar to how intelligence flows from higher to the battalion.

E. NETWORK INTELLIGENCE

1. Networks Defined

The emergence of the network organization follows closely with the need to leverage the full intellectual capital of an organization to solve the critical and complex problems that plague industry in the hypercompetitive marketplace (Quinn, 1996). Networks are uniquely designed to do this, as they are expressly created to seek dominance by being able to bring more talent and brainpower to bear on problem solving, decision making, creative thinking or innovation than rivals can bring to a comparable task. Not a single form of organizing, the network organization is a complex array of fundamentally different organizational forms. At present there are many different network models used throughout industry that bring intellect to bear on varied challenges. Many firms "mix and match" the attributes that best serve their needs. (Quinn, 1996)

While the variety of models prevent the existence of a "typical" network, there are four dimensions that characterize every network organization (Quinn, 1996):

* ❖ *Locus of intellect:* Where the deep knowledge of a firm's particular core competencies primarily lies.
* ❖ *Locus of customization:* Where intellect is converted to novel solutions.
* ❖ *Direction of intellectual flow:* The primary direction in which knowledge flows.
* ❖ *Method of leverage:* How the organization leverages intellect.

One network model, called the Spider's Web by Quinn (1992), is particularly well suited to intelligence. The remainder of this chapter describes how to reengineer the configuration of Marine ground intelligence to derive the powerful advantages offered by the Spider's Web network, thus proposing a possible solution to the major problem posed by this thesis: the pressing need to restructure military intelligence.

2. Applying the Network

The table below presents the dimensions that would characterize military intelligence in its new Spider's Web network form (See Table 7.3).

Structure of Organization:	Net - comprised of internal and external nodes
Example:	The Internet
Locus of Intellect:	Nodes **Internal Nodes:** Battalion, Regiment, Division, MEF **External Nodes:** Media, Academia, Commercial Intelligence, National Level Intelligence
Locus of Customization:	Generation of Intelligence
Direction of Intellectual Flow:	Node to Node
Method of Leverage:	Exponential, Sharing, Expansion

Table 7.3. Marine Ground Intelligence Configured as a Network. After (Quinn, 1992).

In the Spider's Web configuration, the organization is defined as a web like net, comprising interconnecting internal and external **nodes.** **Internal nodes** are those that reside at the intersection where intelligence interfaces with combat decision-makers; internal nodes thus represent the intelligence staff assigned to combat echelons in the Marine Corps (e.g., battalion, regiment, division, MEF, etc.). **External nodes** are those that reside outside of the Marine organization, including both commercial and government intelligence agencies. Commercial nodes include media reporters, private satellite imagery companies, and academics. Government intelligence nodes include the Central Intelligence Agency (CIA), the State Department, the National Security Agency, the National Reconnaissance Office, and the Defense Intelligence Agency, among others.

This model of intelligence **locus of intellect** resides in the nodes, significantly departing from the current intelligence bureaucracy. Here, the intelligence assets and resources are decentralized in the internal nodes rather than centralized in the uppermost level of the hierarchy; in effect, each internal node is a complete intelligence cell uniquely packaged to provide the level of intelligence demanded by the warfighter it supports. In other words, the internal node is a stand-alone intelligence section that can do its own battlefield intelligence collection and analysis without having to rely on the top. The additional locus of intellect residing in external nodes enables intelligence to capitalize on the variety of sources of deep expertise in specific fields related to intelligence, thus offering the organization a wide breadth of knowledge to draw upon.

The **locus of customization** in this model revolves around the generation of intelligence, again a dramatic change from the present organization that revolves around data processing. While individual nodes may operate independently when the problem they face is limited in scope and complexity, they may tap directly into the network (external and other internal nodes) and go beyond their own resources for help when it is essential for them to enlist the intellect of others to solve a more complex problem. When a problem is presented to the net, analysts self-organize into groups, electing participation based on the expertise and value they can contribute to the problem at hand. Once a given problem is completed, the group disbands, and individuals re-form into new groups to address other emerging problems. Thus, the **direction of intellectual flow** occurs between the external and internal nodes of a hierarchy-free network. In this configuration, the **method of leverage** harnesses all three characteristics of intellect: exponentiality, sharing and expansion. Exponentiality is evidenced as each node,

187

particularly internal nodes, gains experience through intimate involvement in problem solving. Sharing is widespread, as contact with even a modest number of collaborating nodes can form knowledge connections that mount into the hundreds or thousands (Quinn, 1996). And expansion is facilitated by the ability of nodes to participate in self-organizing groups that can surge knowledge as necessary.

The figure below depicts an intelligence network operating in accordance with the model being described (See Figure 7.8). Observe how each internal node is connected to every other node throughout the organization. Recall that earlier chapters of this thesis highlighted combat decision-makers' demand for precise intelligence to support maneuver warfare. Now, following this network model, modern day information systems, including the technology that drives the Internet, can make possible the availability of just such intelligence. For example, Internet browsers allow users to download a host of information from a variety of sources, from satellite imagery to newspaper reports. The key to this process is that the users of the Internet themselves select what they need. By contrast, under the present hierarchical intelligence system, formal requests must flow to the top, be approved, processed, and flow back down. Rather than adhering to such slow-moving C2 hierarchies, the internal intelligence node taps directly into the network, enabling to investigate directly into a broad-based platform of information that originates from both classified and open sources.
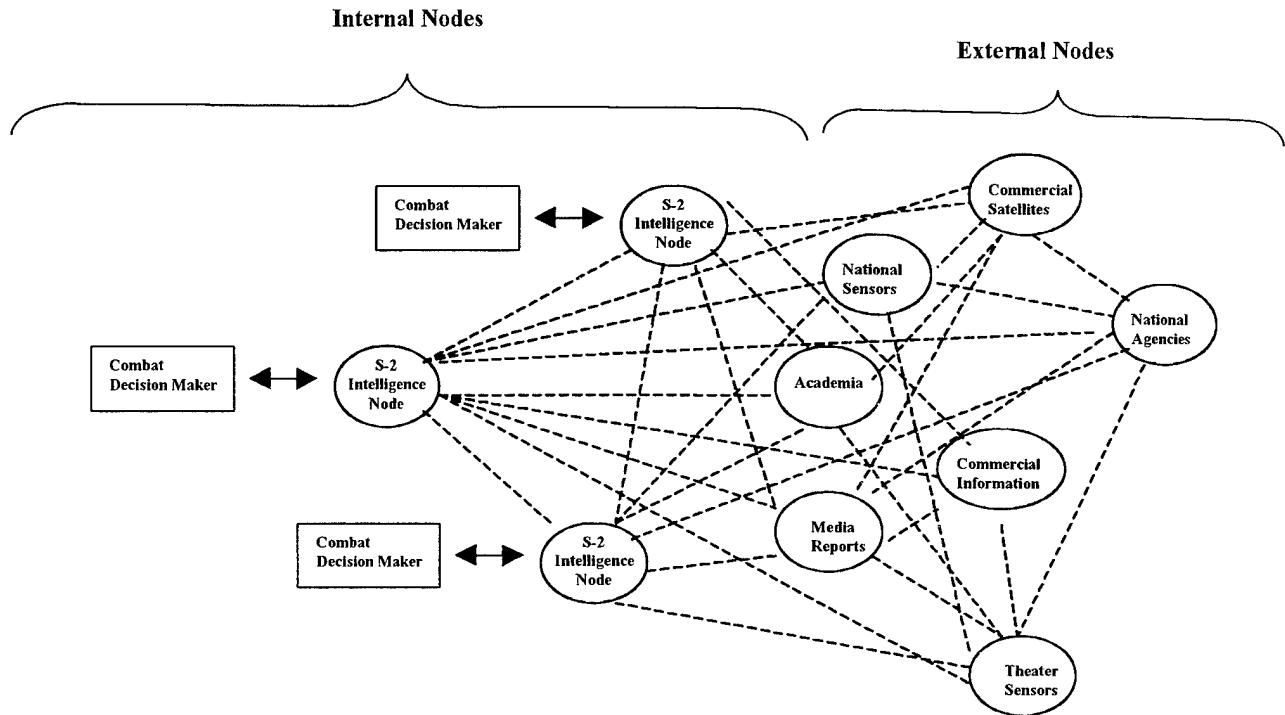
Figure 7.8. The Network Intelligence Architecture.

The intelligence network modeled after Quinn's Spider's Web offers to transform

an information processing intelligence bureaucracy into an agile, intellect-centric

enterprise. With respect to New Order Threats, the Spider's Web design gives

intelligence the form it needs to confront the very type of problem they present, one in

which no single entity knows what the enemy is, how he can be understood, or who may

have potential solutions. By casting a search that drives the work of many different

experts in diverse locations, the net brings together distinct parties in a collaborative

exchange. This approach multiplies the number of possible solutions and leverages the

intellect of a wide variety of experts from many different disciplines.

3. Decentralized Intelligence

Clearly, two fundamental strengths of the network design make it extremely well-suited for the mission of modern Marine ground intelligence: 1) the decentralization of assets and resources to the internal contact nodes to support a highly disciplined focus on customer demands, and 2) the ability to harness the intellect of many different experts in varied fields. A simple example will serve to illustrate the tremendous advantage of converting military intelligence into a decentralized organization.

New York City, Los Angeles, San Francisco, Chicago, Baltimore, and thousands of other big and small cities across the United States all share one thing in common: they only have one to two days worth of food stored in local supermarkets, distribution centers, and warehouses. How then is it that the necessary food is always there? Who determines that the right quantities and varieties are available at the right time and place? The "market" determines these things. Millions of people making independent decisions freely choose what they will sell and buy. The market adjusts, seemingly by a miracle, and the food provided is just what the consumers demand. The thousands of sellers of food learn what their customers need, and they adjust to those demands. A seller of food wanting to meet the demands of the consumer must respond to ever-changing food requirements or get out of the food business.

In contrast, centralized economies like the former Soviet Union do not respond to the same signals as free markets. They sell, produce, and distribute food through a centralized planning process, relying on a central committee to determine what customers want and how it will be distributed. This is a classic problem of centrally planned economies: there are only delayed, weak and fragmentary signals telling producers that

customers are not happy. In other words, regardless of whether the planned offering is what the customer wants or what the market requires, it still gets produced. So, producers keep selling the same centrally planned items, and their products remain the same: stagnant and unresponsive to changing demands. The crux of this problem is that centrally planned organizations cannot possibly adjust to all the market demands they face, because the few central administrators simply cannot digest and process the related mass of information. As a result, the central command's decisions are generally off mark, and the consumer suffers long lines and the lack of availability of the very items they desire.

The market is responsive to the demands of the consumer because economic decisions and power are decentralized. This same concept holds true for intelligence work. The centralized intelligence bureaucracy is not flexible enough to respond to the demands of the organization, and therefore produces a generic, less than desirable product. Decentralization of intelligence assets and resources is critical to providing the level of intelligence demanded by combat decision-makers. The power of decentralizing lies in its focus on the consumer of intelligence. By decentralizing, intelligence nodes have their own resources and assets so that they can probe proactively into their battlespace and produce the intelligence they require. The ensuing reduced information-processing load allows the intelligence agency to transition from a rote-information processing to an intellect-based activity.

The network form dramatically reengineers the distribution of resources and control, configuring each internal node as a self-contained unit equipped with all the assets and personnel necessary to conduct independent intelligence operations. For

example, the intelligence section of an infantry battalion would have its own tactical sensors such as unmanned aerial vehicles, unmanned ground vehicles, and signals intelligence equipment. In addition, a section of analysts would form a fusion center similar to the MAGTF fusion center described in Chapter III.

There are many advantages to this configuration; each revolves around the proximity of intelligence to the combat decision-maker. With the proper tools to probe proactively into the battlespace, intelligence nodes can provide the detailed level of intelligence that warfare by maneuver demands. In the decentralized network configuration, the hierarchy wherein top-level managers evaluate the intelligence needs of the organization and then develop intelligence is replaced with independent nodes of intelligence consumers collecting their own data and processing intelligence based on their own requirements. As the battlefield is fluid and ever changing, the close proximity of intelligence personnel and combat decision-makers facilitates rapid mid-course changes. Finally, combat decision-makers involved in life-or-death situations demand first-hand knowledge. They don't have time to wait for coordinated intelligence to be fused, approved, disseminated, and reworked; they need expert knowledge fast, and decentralized intelligence nodes can perform the analysis quickly and effectively. Furthermore, when knowledge is created, combat decision-makers want to interrogate the analyst; this configuration places all the intelligence assets at the disposal of the combat decision-maker. High-speed analysis is one of the great advantages of decentralized operations.

A second important feature of decentralization is the emergence of intellect-based intelligence work. The problem of information overload has been well documented in this thesis. Decentralization reduces this problem by shifting the intelligence production burden to the internal contact nodes. In this new configuration, the volume and diversity of demands and sensor outputs, by virtue of their distribution across many nodes, is greatly reduced. Each node determines what it will collect and filters incoming data accordingly. The independent self-contained nodes, empowered to collect and select data that is most relevant to their needs, avoid overload by design. The node knows what it can and cannot do, and therefore operates at a level that effectively accomplishes its purpose. Additionally, able to inherently avoid overload, nodes will better leverage intellect to conduct intelligence work. Less concerned with overload, decentralized nodes now have time to conduct the intellectual activity so important to battlefield intelligence. Responding to the demands of a few consumers instead of the entire organization, the nodes can focus their intellectual efforts on critical processes such as threat course of action development. Thus network intelligence is able to reduce information overload, freeing up the organization's intellectual resources to develop knowledge and intelligence and move from an information processing to an intellect-centric activity.

4. Virtual Intelligence

The final aspect of network intelligence to be analyzed is the complex knowledge linkages between nodes. This feature enables the organization to leverage its intellectual producing capacity by a factor of hundreds. Many of the links between nodes cross great geographic distances, achieving the concept of virtual intelligence, where knowledge

need not be co-located with its clients (forward-deployed forces). In other words, virtual intelligence exploits information technology and communication systems in order to leverage a wide body of geographically separated experts through networked collaboration. With this configuration, the internal contact node benefits from the expertise and insight of a wide breadth of expert knowledge. In sum, the many specialists that are made active participants during the network's collaborative exchanges augment the internal nodes' limited expert knowledge. In today's threat environment this is critically important, as the enemy is less likely to be understood, and solutions will require the knowledge of experts from many different disciplines.

The network design has its own potential drawbacks, however. The rich knowledge that the network produces can easily cause information overload. As intellect and knowledge become the most important resources in combating New Order Threats, it is increasingly imperative that the widest body of knowledge is available for analysis. Every relevant piece of information adds to a more complete understanding and aids in gaining an advantage over an adversary. But sifting through the mountains of generated material risks complete inundation and overload. The answer to this overload problem resides within the nature of the network. Through practice and experience, nodes will learn how to participate and deliver succinct knowledge in easily understandable forms. In other words, the internal nodes will learn how to use the system to avoid information overload. This somewhat soft solution to the network problem is not without precedent.

Silicon Graphics,[5] a leading manufacturer of state of the art computer equipment, has a networked system in place for knowledge generation. Employees are allowed unlimited access to the Internet and use it as a resource to collect intelligence on competitors and to form collaborative working groups to solve complex problems. The CEO described the access employees have to the wealth of information age knowledge as phenomenal. He explained that at first, employees are consumed and inundated by the tidal wave of knowledge the Internet unleashes - so consumed that for the first several weeks they may even neglect their assigned tasks. However, after a short initiation period, workers become savvy about the most effective ways to harness the web. Instead of surfing for long periods of time and bouncing around a multitude of sites, users learn which sites are most helpful and frequent them deliberately. Furthermore, workers identify and subscribe to services that deliver information based on customized topic lists. While information overload may indeed pose a problem, the network configuration empowers people to direct their searches themselves and ultimately learn to avoid overload and harness the network to their advantage.

The potential for overload may be further mediated by advances in information technologies. One approach would be for intelligence to employ sophisticated browser interfaces similar to the Internet. As different operating environments demand different levels of intellect creation and interaction, different interfaces may need to be created. For example, in a fast-paced combat situation, external nodes like national and theater assets could combine with internal nodes and create a map sheet of the combat area on a web page. Together, national nodes could place intelligence from national systems,

[5] This is taken from comments given by the CEO of Silicon Graphics at a guest lecture given at the Naval Postgraduate School in August of 1996.

theater analysts could place intelligence from theater systems, and other internal nodes could place their specific intelligence on the web page to build an enemy situation map in real time - enabling the product to be instantaneously disseminated.

In a less fast-paced environment, like Somalia, external nodes like economists and academics could post generated knowledge on a web page. Internal contact nodes could then scan and selectively choose what they needed. Recall that the network revolves around the internal contact nodes; they work to provide maneuver warfare intelligence for combat decision-makers and are accordingly the focal point for all organizational knowledge creation. In effect, the organization sits dormant until the internal nodes query the intellect of the network. Therefore, as a battlefield situation develops, the nodes inform the network as to what is going on and direct queries for knowledge as required. The network is then activated, and experts form into self-generating groups to tackle the problems confronted by the contact node.

One of the most powerful aspects of the network is that ground intelligence can reach outside its organization to acquire knowledge. Twenty-first century ground intelligence cannot be limited to narrow analysis by focusing only on traditional intelligence sources like organic, theater, and national assets. As demonstrated by the Somali case study, New Order Threats are complex and difficult for traditional intelligence sources to detect. Left undetected, they leverage asymmetry to garner tremendous battlefield advantage. Aideed's powerful militia remained an unrecognized force until Mogadishu exploded in violence in October of 1993. Could other experts have helped intelligence professionals on the ground see a more complete picture than what their sophisticated sensors were able to reveal? Could an economist, social

scientist, expert on African internal affairs, and a media representative have contributed to building a more realistic intelligence picture of the situation on the ground in Somalia? An important premise of the intelligence network is that government does not have a monopoly on intelligence work, that the commercial environment offers tremendous knowledge generating capabilities. There exists more regional expertise and knowledge on weapons and computer information systems in the civilian sector than in government, and this is increasingly more true with every passing year.

The network allows these experts, geographically separated, to work collaboratively in support of internal contact nodes that may be presented with complex battlefield problems that demand expert attention. The network facilitates academics, media representatives, analysts at the CIA or DIA, and business leaders to contribute to virtual, self-organizing teams simply by sitting at their own desks. In this model, an internal contact node communicates a need across the network. Using advanced information technologies, the network uses knowledge about each analyst's work profile to distribute the need to the right people. Experts spread across the network signal their wish to participate and join in, contributing their expertise to knowledge creation. One expert may have relevant imagery, while another may have some socio-political analysis to contribute. Together with the internal contact node, the experts work to create knowledge. This system relies on individual experts, spread across government, industry, and academia to make the initial judgments as to whether their expertise matches the problem at hand. The degree to which they then contribute is determined by how fast the consumer needs an answer. The key to the collaborative network is that experts with a breadth of knowledge self organize into collaborative teams that can respond with great

flexibility and agility to the demands of the consumer. This expert knowledge can then be applied to gain that ever so slight advantage over an increasingly more powerful and sophisticated enemy.

F.   SUMMARY

This chapter began by identifying the most important characteristic of ground intelligence: intellect and its deployment. New Order Threats were juxtaposed with threats of the past to demonstrate the importance, now more than ever, of intellect-based intelligence. Intellect, however, was shown to have particular requirements for its cultivation. Successful leveraging of intellect in the intelligence organization demands reengineering that would focus the organization on intellectual processes and match those processes with a design that best leverages them. The three key characteristics of intellect, exponentiality of knowledge, the benefits of sharing, and the opportunities for expansion, were described to be critical to any organization seeking to successfully exploit its resident brainpower. A broad level value chain analysis was used to demonstrate that rote information processing, not intellect-centric activity, characterizes modern day ground intelligence work. Additionally, the complementary interface between man and machine demanded by information age intelligence work was demonstrated to be dysfunctional because of information overload, with machine work dominating the intelligence process and relegating it to data processing.

The key to intellect-centric operations was shown to be designing the organization around intellectual flows rather than around command and control concepts. For intelligence, this entailed abandoning the attrition era C2, which is incompatible with the demands of intellect based intelligence. The detail and complexity of information age

intelligence was illustrated as clogging attrition era command and control infrastructures and overwhelming the system and operators alike. New technologies and successful experiences in industry were used to shed light on how to reorganize intelligence around intellectual flows. The *network organization* was identified as the emerging form that accomplishes this reorganization by incorporating web-based technologies and organizational design. The network form clearly pushes responsibility outward, flattens and removes hierarchy, is faster and more responsive to the demands of the customer, and is agile to adapt to a chaotic and ever changing environment. In contrast to the intelligence bureaucracy, the main function of the network organization is to develop and deploy (i.e. attract, harness, leverage, and disseminate) intellect effectively (Quinn, 1996). (See Table 7.4).

	Intelligence Bureaucracy	Network Intelligence
Nature of Design	Centralized –Hierarchical	Decentralized –Web-like
Key part of organization	The Top	The Nodes
Method of Work	Standardization	Intellect and Collaboration
Key activity	Information-Processing	Intellectual Processing with Man-Machine interface
Flow of Decision Making	Top Down	Mixed, all levels
Flow of Authority	Top Down	Insignificant
Flow of informal communication	Discouraged	Significant throughout
Control Systems	Significant	Insignificant
Environment	Simple and stable	Complex and dynamic

Table 7.4. Comparison Between Organizational Forms of Intelligence.

Quinn's Spider Web was presented as the network form that best suits ground intelligence. Two of its most salient features are ideally suited for intelligence: the decentralization of assets and resources to the internal contact nodes to support a highly

disciplined focus on customer demands, and the ability to harness the intellect of many different experts in varied fields.

Network intelligence was modeled with each contact node configured to be a self-contained unit, providing the crucial advantage of decentralization to allow for proactive inquiry into the battlespace, a key element to effective intelligence support for maneuver warfare. Other advantages of the model include the ability of intelligence nodes to make mid-course changes and rapidly generate tailored intelligence. Perhaps the most important outcome of decentralization is the shift from rote-based information processing to intellect-centric work. The decentralized model was shown to reduce information overload and free intellectual resources to develop knowledge, producing intelligence rather than reworked data.

The network configuration also evidenced the capability to achieve virtual intelligence, the concept that knowledge need not be co-located with forward-deployed forces, by permitting collaboration between geographically separated experts from the military, government, and private sector. This collaboration is an important feature of the network, as New Order Threats are less likely to be understood by the narrow analytical ability presently afforded to ground intelligence. Much debate has focused on the potential for network overload; however, in this chapter the nature of the network was shown to be able to preclude overload. Through practice and experience, nodes were shown to be able to dynamically learn how to best function to avoid overload and maximize the capabilities of the system.

Intellect is the cornerstone to successful ground intelligence work. In a previous age, when threats mirrored the Soviet model and clung to regimented tactics and

centralized C2, sophisticated sensors could provide all the answers. However, in the emerging environment, threats are increasingly less centralized and regimented. They think on their own, and they adapt quickly. To counter these smart adversaries Marine intelligence will need to look vastly different from the way it does now. It must be organized around and designed to enhance the deployment of intellect. Information systems aid in the collection of information and the delivery of intellect, but they are not intellect unto themselves. People, fed critical battlefield information in a timely fashion, deploy intellect. Attrition era intelligence practices and C2 organization must be abandoned if intellect and its deployment are to shape future Marine operations. In sum, Marine intelligence must be designed to be an agile, networked enterprise. Configured with the right tools, organized around intellect and its deployment, Marine operations demand an intelligence function that can provide that ever so slight advantage over an increasingly more powerful and sophisticated enemy.

VIII. CONCLUSION AND FUTURE WORK

A. CONCLUSIONS

This thesis has sought to answer three broad questions. First, what is the emerging threat environment of the twenty-first century? Second, is the present Marine ground intelligence design adequate to support combat decision-makers in this threat environment? Third, if not, what design changes are necessary to align intelligence with this environment?

This thesis argues that Marine ground intelligence is improperly configured to provide the intelligence required by maneuver warfare and to operate effectively against the emerging threats of the next century. This work shows that, ill configured for threats like the Iraqi Army, Marine ground intelligence will assuredly fail against emerging twenty-first century threats that are asymmetric and adaptive. The restrictive boundaries, formalized processes, regimented hierarchical approach to collections and dissemination, and the centralization of assets and resources prevents Marine ground intelligence from organizing properly to fulfill its critical mission. Unless significant change is realized, Marine intelligence faces a serious dilemma: it can either reform or face ever decreasing relevance and effectiveness as a central component of command and control on the battlefield.

This work demonstrates that Marine ground intelligence fits the pattern of a machine bureaucracy that is centralized, hierarchical and slow. Designed to accommodate attrition warfighting and simple, predictable adversaries, Marine intelligence is severely

challenged when confronted with the demands of maneuver warfare and non-standard, unpredictable *New Order Threats*.

Maneuver warfare places overwhelming demands on the intelligence bureaucracy. Proactive inquiry floods the central intelligence cell with demands for information age intelligence, overloading the system and reducing its processing capability. With all the tools for collecting intelligence at the top, lower echelons are left without intelligence. As a result, tactical units do not receive intelligence when they require it, forcing them into attritionist tactics.

The *New Order of Threat* environment also severely challenges the Marine intelligence bureaucracy. New Order Threats assert this challenge because they are difficult to recognize and understand. Because of their unique nature, these threats, unlike other forms of warfare, are not expressly tied to a specific form of operations. This fact strains modern threat assessment. Marine intelligence is designed to accommodate simple, predictable adversaries; its present day intelligence methods and systems are rendered ineffective by these threat operations. Consequently, New Order Threats place intelligence in a quandary that results in delay or ineffective response. Left unchecked, New Order Threats harness powerful asymmetric capabilities that allow them to gain influence that is out of proportion to their political, economic, and military strength.

The case examples drawn from actual and hypothetical military encounters in Somalia and Taiwan, as well as low and mid-order threats like U.S. street gangs and drug Cartels, all illustrate that asymmetric and emerging non-conventional threats are posing greater complexity and will overwhelm a bureaucratic intelligence enterprise configured for the past. These emerging *New Order Threats* are networked, unconventional, agile,

adaptable, evolving, asymmetric, non-linear and configured to operate across the political, economic and mass media spectrum.

In a previous age, when threats mirrored the Soviet model and clung to regimented tactics and centralized command and control, intelligence practices heavily reliant on sophisticated sensors to provide all the answers, worked. However, in the emerging environment, threats are increasingly less centralized and regimented. They think on their own and they adapt quickly. To counter these smart adversaries, Marine ground intelligence must move from a rote information processing machine bureaucracy to an intellect-centric network organization.

The key to the network organization is the focus on intellectual processes rather than command and control concepts. The network pushes responsibility and control over resources outward, flattens and removes hierarchy, is faster and more responsive to the demands of decision-makers and is agile to adapt to a chaotic and ever changing environment. The main function of network intelligence, therefore, is to develop and deploy intellect against complex and difficult problems created by the demands of maneuver warfare and *New Order Threat* operations.

Network intelligence decentralizes assets and resources to the internal contact nodes allowing for a highly disciplined focus on the demands made by combat decision-makers. Decentralization allows for proactive inquiry into the battlespace, a key element to effective intelligence support for maneuver warfare. Other advantages include the ability to make mid-course changes and rapidly generate tailored intelligence. Perhaps most importantly, decentralization allows for a shift from rote-based information processing to intellect-centric work. Decentralization reduces information overload freeing

up intellectual resources to develop knowledge. The end product is intelligence not reworked data.

The network also harnesses the intellect of a multitude of experts in varied field and allows them to surge brainpower on critical problems. This focused collaboration is important, as *New Order Threats* are less likely to be understood by the narrow analytical ability found within Marine intelligence. To understand and predict against these threats demands an organization that can leverage the intellect of experts from many fields within the military, government and private sector. Thus, the virtual deployment of a wide field of intellectual resources to solve complex problems is a key component of the network intelligence enterprise.

Intellect is the cornerstone to successful ground intelligence work. Intellect however is not easy to cultivate and harness. Successful leveraging of intellect demands reengineering that focuses the organization on intellectual processes and matches those processes with a design that best leverages them. Marine ground intelligence is ill configured to leverage its resident intellectual resources. So far, in recent operations, the individual innovation and "get the job done" attitude of intelligence personnel have averted disaster through work-arounds.

Interestingly, high-level combat decision-makers do not tolerate the "unworkableness" of their intelligence support. They therefore unknowingly push them into informal network-like relationships to prevent the issues that really count from slipping through the cracks. However, these "quick fixes" are rarely formalized by the organization. There remains an official way to do intelligence, and then there is the unofficial way things are done in crises. This manner of operations may have been

sufficient for the past, but the new "order of things" promises to seriously challenge these ill-configured and misaligned practices in the future.

B. RECOMMENDATIONS FOR FUTURE WORK

This thesis is intentionally short on detailed system descriptions or engineering analysis of information systems because the decision to correct the shortcomings of the current configuration will not be made by engineers but by leaders of Marines. Accordingly, this work has been an effort to suggest an alternative approach to ground intelligence; an approach centered around the complimentary interface between human intellect and machine instead of one exclusively focused on sensor and machine processes. Much work is required to bring the promise of network-centric intelligence design and practices to Marine ground intelligence.

First, a collaborative partnership needs to be established with industry and academia to harness the power and potential of intellect and network centric designs that are coming to the forefront of modern business practices and academic research. Next, these designs and practices must be prototyped at the lowest levels within the ground operational force. Real-world statistics should be collected and a thorough analysis conducted under near combat conditions to assist combat decision makers in determining the viability and effectiveness of such radical change. Furthermore, this field testing is essential to convince battlefield commanders of the utility of intellect-centric intelligence and the power of the network intelligence enterprise.

An important component of the network intelligence enterprise is its adaptiveness and agility. It must be understood that as a decentralized form of operations, each internal node must be given the resources and freedom to innovate and adapt the nodes

organizational design to best satisfy the needs of his commander. This is key as the ability to proactively inquire into the battlespace and identify threat asymmetries, an important component in developing preemptive options, demands this level of innovation and agility.

This suggests that an important component to network success is advanced information technologies. In other words, the network organization demands capable and powerful information systems.

Advances in information technologies have exploded in the last fifteen years. What used to take twenty years to develop now takes eighteen months or less. Many argue that hypercompetition in the information technology area is spawning mini-technical revolutions. They state that every year monumental breakthroughs occur in high technology computing that make the transition from vacuum tube based computers to silicon circuit computers, pale in comparison. Regardless of the commentary, it is understood that many information technologies are outdated eighteen months after they are introduced. After eighteen months hardware is obsolete and software upgrades are no longer available.

The challenge for Marine ground intelligence will be to tap into the cutting edge of information technology while operating within the constraints of DoD's bureaucratic budgetary and acquisition systems. Maintaining the technological lead necessary for twenty-first century ground intelligence operations will not be cheap. Resources must be spent wisely to avoid unncessary waste. A concerted effort must be made in redesigning intelligence acquisition so that the right tools are placed into the hands of intelligence professionals quickly and within the constraints of the current fiscal environment. The 10-15 year acquisition cycle, a symbol of Cold War era operations, cannot continue to be the

way things are done. This process must be reformed and acquisition cycle times must be configured to be more in step with technological revolutions instead of bureacuratic ones. Therefore a significant challenge for Marine Corps ground intelligence will be to harness the revolution in information technology occurring in private industry and leverage it to aid in maintaining that ever so slight analytical advantage required for operating succesfully in the current operating environment.

Specific recommendations for future work follow.

1. The Network Organization

a. Decentralization

(1) Determine how to best organize and equip the internal intelligence node of the battalion, regiment and division.

(2) Determine the security ramifications of decentralized operations.

(3) Explore information technologies that can assist in disseminating intelligence from the intelligence node to lower combat echelons.

b. Virtual Intelligence

(1) Investigate how to best establish a network of experts that spans across military, academic and industry.

(2) Study the security ramifications of virtual operations.

(3) Explore information technologies that can best leverage this manner of operations.

c. The Innovative and Agile Intelligence Enterprise

(1) Determine the organizational changes in structure and technology to enhance innovation and agility within the internal nodes.

(2) Research industry examples of innovative enterprises like Intel,GE and Silicon Graphics and investigate how their focus on innovation can be applied and incorporated within ground intelligence.

APPENDIX A. MAJOR-ARMED CONFLICT VS. INTERNAL DISPLACEMENT AND REFUGEE DATA

Nations experiencing Major Armed Conflict (Source SIPRI)		Nations experiencing Internal Displacement (Source IFRC)	
Bosnia-Herzegovina	Guatemala	Angola	Panama
Croatia	Peru	Burundi	Peru
Chechnya		Djibuti	Ecuador
Iran		Eritrea	Afghanistan
Iraq		Ethiopia	Cambodia
Israel		Kenya	India
Turkey		Liberia	Myanmar
Afganistan		Mozambique	Philippines
Bangladesh		Rwanda	Sri Lanka
Cambodia		Sierra Leone	Tajikistan
India		Somalia	Azerbaidjan
Indonesia		South Africa	Bosnia Herzegovina
Myanmar		Sudan	Croatia
The Philippines		Togo	Serbia
Sri Lanka		Uganda	Cyprus
Tajikistan		Zaire	Georgia
Algeria		Colombia	Moldovia
Angola		El Salvador	Yugoslavia
Liberia		Guatemala	Chechnyia
Sierra Leonne		Haiti	Iran
Somalia		Honduras	Iraq
Sudan		Nicaragua	Yemen
Colombia		Turkey	Lebanon
Total:		**Total:**	
Major Armed Conflict*	**25**	**Internal Displacement**	**46**

*The total annual number of conflicts does not necessarily correspond to the number of conflict locations in table 1.00 in Chapter 4, since there may be more than one major armed conflict in each location.

Appendix Table 1.1. Major Armed Conflict vs. Internal Displacement.

Nations experiencing Major Armed Conflict (Source SIPRI)		Nations experiencing Cross Border Refugee Problems (Source IFRC)	
Bosnia-Herzegovina		Algeria	South Africa
Croatia		Angola	Sudan
Chechnya		Benin	Swaziland
Iran		Botswana	Tanzania
Iraq		Burkina Faso	Togo
Israel		Burundi	Tunisia
Turkey		Cameroon	Uganda
Afganistan		Central African Republic	Zaire
Bangladesh		Congo	Zambia
Cambodia		Cote dIvoire	Zimbabwe
India		Djibouti	Armenia
Indonesia		Egypt	Austria
Myanmar		Ethiopia	Azerbaidjan
The Philippines		Gabon	Belarus
Sri Lanka		Gambia	Bosnia-Herzegovina
Tajikistan		Ghana	Croatia
Algeria		Guinea	Czech and Slovak Rep
Angola		Guinea-Bissau	Hungary
Liberia		Kenya	Macedonia
Sierra Leonne		Lesotho	Romania
Somalia		Liberia	Yugoslavia
Sudan		Malawi	Bahrain
Colombia		Mali	Gaza Strip
Guatemala		Mauritania	Iran
Peru		Morocco	Iraq
		Mozambique	Jordan
		Namibia	Lebanon
		Niger	Syria
		Nigeria	West Bank
		Rwanda	Afghanistan
		Senegal	Bangladesh
		Sierra Leonne	India
		Somalia	Kazakhstan
Total:		Total:	
Major Armed Conflict*	25	Refugee Countries	66

*The total annual number of conflicts does not necessarily correspond to the number of conflict locations in table 1.00 in Chapter 4, since there may be more than one major armed conflict in each location.

Appendix Table 1.2. Major-Armed Conflict vs Refugee Data by Host Country.

LIST OF REFERENCES

Arquilla, John, and David Ronfeldt. The Advent of Netwar. Santa Monica, CA: RAND, 1996.

Atkinson, Rick. "The Raid that Went Awry", Washington Post, January 30, 1994.

_____. "Night of a Thousand Casualties", Washington Post, January 31, 1994.

Berkowitz, Bruce D. "Information Age Intelligence." Foreign Policy, 1996.

_____. "Information Technology and Intelligence Reform." Orbis, Winter 1997.

_____. Unpublished Book. 1997.

Binnendijk, Hans, ed. 1997 Strategic Assessment. Washington D.C: National Defense University, 1997.

Blank, Stephen. Responding to Low-Intensity Conflict Challenges. Maxwell Air Force Base, AL: Air University Press, 1990, 53-125.

Brooks, John R. "Things Are A-Changin: The Results of the TF XXI are in." Military Intelligence, July-September, 1997.

BSTF (Battle Staff Training Facility). Strategic Plan and Related Documents. Marine Corps University, Quanitco VA: Unpublished Draft Document, 1997.

Bunker, Robert J. "The Transition to Fourth Epoch War." Marine Corps Gazette, September 1994.

_____. "Epochal Change: War Over Social and Political Organization." Parameters, Summer 1997.

_____. "Internetted Structures and C2 Nodes." Military Intelligence, April 1996.

Byrne, John A. "The Virtual Corporation." Business Week, February 8, 1993.

_____. "The Horizontal Corporation." Business Week, December 20, 1993.

Campen, Alan D. The First Information War. Fairfax, VA: AFCEA International Press, 1992.

Casper, Lawrence E. et al. "Knowledge Based Warfare: A Security Strategy for the Next Century." Joint Forces Quarterly, Autumn 1996.

_____. "Summary of Combat Operations on 3 October: QRF, Falcon Brigade, 10th Mountain Division" Unpublished After Action Report. 1994.

David, Ruth A. "The Agile Intelligence Enterprise." Unpublished Article.

Driver, Michael J, et al. The Dynamic Decision Maker: Five Decision Styles for Executive and Business Success, 1990.

Dess, Gregory G. et al. "The New Corporate Architecture." Academy of Management Executive, Vol. 9 Number 3, 1995.

Farah, Douglas, "Drug War Breaks Out in Mexico." The Washington Post, July 23, 1997.

_____. "Russian Mob, Drug Cartels Joining Forces." The Washington Post, September 29, 1997.

Galbraith, Jay. Organization Design. Menlo Park, CA: Addison-Wesley Publishing Co., 1977.

_____. "The Innovating Organization." Organizational Dynamics, Winter 1982, 5-25.

_____. Designing Complex Organizations. Reading, MA: Addison-Wesley Publishing Co., 1973.

Gordon, Michael R, and Bernard E. Trainor. The Generals' War. New York: Little, Brown and Company, 1995.

Hammes, Thomas X. "The Evolution of War: The Fourth Generation." Marine Corps Gazette, September 1994.

Headquarters, Department of the Army. FM 34-3 Intelligence Analysis. Washington D.C: 1990.

_____. FM 34-130 Intelligence Preparation of the Battlefield. Washington D.C: 1993.

Headquarters, United States Marine Corps. FMFM 3-21 MAGTF Intelligence Operations. Washington D.C: 1991.

_____. MCDP 6 Command and Control. Washington D.C: 1996.

_____. MCDP 2 Intelligence. Washington D.C: 1997.

Holmes, Kim R. and Thomas G. Moore, ed. Restoring American Leadership: A U.S. Foreign and Defense Policy Blueprint. Washington D.C: The Heritage Foundation, 1996.

Huntington, Samuel P. The Clash of Civilizations and the Remaking of World Order.
     New York: Simon and Schuster, 1996.

International Federation of Red Cross and Red Crescent Societies. World Disasters
     Report 1997. New York: Oxford University Press, Inc., 1997.

Lewin, Ronald. The Life and Death of the Afrika Korps. New York: Quadrangle, 1997.

Lind, William S. et al. "The Changing Face of War: Into the Fourth Generation." Marine
     Corps Gazette, October 1989.

Lopez, Robert J. "Broader Anti Gang Plan Sought." Los Angeles Times, November 27,
     1996.

_____. "An Inside Look at 18th Street's Menace." Los Angeles Times, November 17,
     1996.

_____. "Gang Turns Hope to Fear, Lives of It's Victims to Ashes." Los Angeles Times,
     November 18, 1996.

_____. "Gang Finds Safe Haven and Base for Operations in Tijuana." Los Angeles
     Times, November 19, 1996.

_____. "Multifaceted Response to 18th Street Gang Urged." Los Angeles Times,
     November 21, 1996.

Luttwak, Edward N. "Toward Post-Heroic Warfare." Foreign Affairs, May-June 1995.

Macgregor, Douglas A. Breaking the Phalanx: A New Design for Landpower in the 21st
     Century. Westport, CT: Praeger Publishers, 1997.

Metz, Helen C. Somalia: A Country Study. Headquarters, Department of the Army,
     1993.

Marine Corps Intelligence Activity. Threats in Transition. Washington D.C:
     Headquarters, USMC, October 1994.

Millet, Alan R. and Williamson Murray. Innovation in the Interwar Period. Washington
     D.C: Office of Net Assessment, The Pentagon, 1994.

Mintzberg, Henry. Structure in Fives. Englewood Cliffs, NJ: Prentice Hall, 1993.

National Drug Intelligence Center. National Street Gang Survey Report. Jonestown, PA:
     U.S. Department of Justice, 1996.

Operation Safe Streets. <u>L.A. Style: A Street Gang Manual of the Los Angeles County Sheriff's Department.</u> Los Angeles: Unpublished, 1994.

Peters, Ralph. "The New Warrior Class." <u>Parameters,</u> Summer 1994.

Pillsbury, Mike. "Asia 2020: The Future Asian Security Environment." Washington D.C: Unpublished, Prepared for the Director of Net Assessment, Office of the Secretary of Defense, 1993.

Quinn, James Brian. <u>Intelligent Enterprise.</u> New York: The Free Press, 1992.

_____. "Leveraging Intellect." <u>Academy of Management Executive,</u> Vol. 10 Number 3, 1996.

Rosen, Stephen. <u>Winning the Next War: Innovation and the Modern Military.</u> Ithaca, NY: Cornell University Press, 1991.

Schmitt, John F. "What is an Intelligence Failure?" <u>Marine Corps Gazette,</u> October 1997.

Schneider, Barry R. and Lawrence E. Grinter. <u>Battlefield of the Future.</u> Maxwell Air Force Base, AL: Air University Press, 1995, 5-43.

Segal, Gerald. "How Insecure is Pacific Asia?" <u>International Affairs,</u> Vol. 73,2, 1997.

Stockholm International Peace Research Institute (SIPRI). <u>SIPRI Yearbook 1995.</u> Oxford University Press, London, 1995.

_____. <u>SIPRI Yearbook 1996.</u> Oxford University Press, London, 1996.

Stavridis, James. "The Second Revolution." <u>Joint Forces Quarterly,</u> Spring 1997.

Steele, Robert D. <u>Intelligence Preparation of the Battlefield: the Marine Corps Viewpoint.</u> Washington D.C: Headquarters, USMC, C4I, 1992.

Thayer, Nate. "Drug Suspects Bankroll Cambodian Coup Leader." <u>The Washington Post,</u> July 22, 1997.

The International Institute for Strategic Studies (IISS). <u>The Military Balance 1996/1997.</u> Oxford University Press, London, 1996.

Toffler, Alvin and Heidi. <u>War and Anti War.</u> New York: Warner Books Inc., 1993.

Turner, Albert F. "On the Path to the Digital Division: Force XXI and the AWEs." <u>Military Intelligence,</u> July-September, 1997.

Van Creveld, Martin. The Transformation of War. New York: The Free Press, 1991.

_____. Technology and War. New York: The Free Press, 1989.

_____. Command in War. Cambridge, MA: Harvard University Press, 1985.

Van Riper, Paul K. "Information Superiority." Marine Corps Gazette, June 1997.

Watts, Barry D. Clausewitzian Friction and Future war. Washington, D.C: Institute for National Strategic Studies, National Defense University, 1996.

The World Bank. World Development Report 1995. New York: Oxford University Press, Inc., 1995.

_____. World Development Report 1996. New York: Oxford University Press, Inc., 1996.

INITIAL DISTRIBUTION LIST

No. of copies

1. Defense Technical Information Center..2
   8725 John J. Kingman Road, Ste 0944
   Ft. Belvoir, Virginia 22060-6218

2. Dudley Knox Library..2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, California 93943-5101

3. Director, Training and Education..1
   MCCDC, Code C46
   1019 Elliot Rd.
   Quantico, Virginia 22134-5027

4. Director, Marine Corps Research Center..2
   MCCDC, Code: C40RC
   2040.Broadway Street
   Quantico, Virginia 22134-5107

5. Director, Studies and Analysis Division 1
   MCCDC, Code C45
   3300 Russell Road
   Quantico, Virginia 22134-5130

6. Marine Corps Representative...1
   Naval Postgraduate School
   Code 037, Bldg. 234, HA-220
   699 Dyer Road
   Monterey, CA 93940

7. Marine Corps Tactical Systems Support Activity..1
   Technical Advisory Branch
   Attn: Maj J.C. Cummiskey
   Box 555171
   Camp Pendleton, CA 92055-5080

8. Captain Drew Cukor 5
   Marine Corps Systems Command
   203 Barnett Avenue, Suite 315
   Quantico, Virginia 22134-5010

9. Prof. Nancy Roberts, Code SM/RC..1

10. Prof. Erik Jansen, Code SM/EK 1